Universidade de Aveiro
Departamento de
Electrónica, Telecomunicações e Informática,
2010

Marcelo Lebre
da Silva

TRANSPORTE DE CONTEXTO BASEADO NO PROTOCOLO 802.21

Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática,
2010

Marcelo Lebre da Silva

TRANSPORTE DE CONTEXTO BASEADO NO PROTOCOLO 802.21

"If you want to make an apple pie from scratch you must, first, invent the Universe."

Carl Sagan

Marcelo Lebre da Silva

TRANSPORTE DE CONTEXTO BASEADO NO PROTOCOLO 802.21

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Computadores e Telemática, realizada sob a orientação científica de Rui Aguiar, Professor do Departamento de Electrónica Telecomunicações e Informática da Universidade de Aveiro e Diogo Gomes, Professor do Departamento de Electrónica Telecomunicações e Informática da Universidade de Aveiro.

o júri / the jury

presidente / president

Prof. Dr. João Nuno Matos
Professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

vogais / examiners committee

Prof. Dr. Diogo Gomes
Professor assistente convidado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro (orientador)

Prof. Dr. Rui L. Aguiar
Professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro (co-orientador)

Prof. Dr. Jorge Sá Silva
Professor auxiliar da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

agradecimentos / acknowledgements

A elaboração e conclusão desta dissertação terminou uma pequena etapa de muitas. O sucesso da mesma deve-se, em grande parte, à disponibilidade de todos os que contribuíram para que os objectivos associados fossem cumpridos.
Agradeço ao professor doutor Rui Aguiar pela oportunidade para desenvolver todo este trabalho, ao professor doutor Diogo Gomes pelo tempo dispêndido, pela sabedoria partilhada e pelas respostas às minhas questões sempre tão céleres, ao engenheiro Daniel Corujo cuja pronta, constante e apreciada disponibilidade se tornou num suporte essencial ao trabalho desenvolvido. Quero também agradecer ao grupo de pessoas que compõe o HNG, o ODTONE e o PT *Context Broker* pela colaboração e assistência.
Finalmente, argradeço aos meus pais, avós, irmã, namorada e amigos, não só pelo contínuo e incontestável apoio, mas sobretudo pela paciência.

Dedico esta dissertação ao meu Avô.

Palavras Chave

802.21, Adaptação, Contexto, Plataformas de gestão de contexto, Redes de Sensores, Redes Heterogéneas, XMPP

Resumo

Num mundo onde a conectividade e informação são constantes do quotidiano, torna-se pertinente questionar qual o próximo passo. Até agpra o desafio centrava-se nos mecanismos e formas de conseguir fornecer aos utilizadores os meios para uma conectividade ininterrupta disponibilizando ao mesmo tempo uma panóplia de serviços de informação que acomodassem as necessidades de todos. Agora que ambas condições se verificam como dado adquirido, o próximo passo será adaptar a conectividade e a forma como a informação é oferecida aos utilizadores, de uma forma puramente transparente, tendo em conta as suas preferências, gostos e necessidades.
A avaliação das apreciações, opções, estados e equipamentos de um utilizador, bem como o ambiente em que se encontra, permite a caracterização lógica do seu contexto. Através da análise contexto de um utilizador é possível inferir alguns dos seus hábitos, prever alterações de utilização e efectuar decisões/escolhas automaticamente sobre questões como a conectividade e a alteração do comportamento da aplicação consoante o ambiente em redor, personalizando e adaptando a utilização às condições que rodeiam e compõe o utilizador.
As redes de sensores são valiosas fontes de informação uma vez que fornecem informação adicional que os dispositivos por norma não têm acesso. Por este motivo, as redes de sensores são consideradas uma das maiores e melhores fontes de informação do ponte de vista da análise de contexto.
Numa rede heterogénea, podem encontrar-se redes de tecnologias completamente diferentes (e.g. WiFi, WiMAX, 3G, etc.), um dos problemas recorrentes é encontrar um ponto comum a todas essas tecnologias que permita uma navegação e experiência contínua. A norma 802.21 é o ponto comum entre várias tecnologias, embora a sua finalidade principal seja facilitar o *handover* das comunicações entre duas redes, pode operar ao nível da camada dois e aceder a informação que normalmente só estaria disponível na camada três. Nesta dissertação demonstrar-se-à como aproveitar a vantagem desta camada 2,5 para aceder e disponibilizar informação de contexto.
O transporte de contexto baseado em 802.21 propõe-se a abordar estes conceitos através de um demonstrador, que engloba uma cooperação entre a norma 802.21, plataformas de gestão de contexto (serviços de informação) e redes de sensores, com o objectivo de facilitar a personalização de aplicações e dispositivos de uma forma automática e transparente para o utilizador.

Keywords 802.21, Adaptation, Context, Context Management Platforms, Heterogeneous Networks, Sensor Networks, XMPP

Abstract

In a world where connectivity and information are constants in our everyday, the question about what is going to be the next step becames more and more relevant. Until now the challenge was focused on the mechanisms and procedures that would provide the users with the means to obtain an uninterrupted connectivy and experience at the same time that a huge panoply of information services capable to accommodate user needs was made available. Now that those two features are reality, the next step starts to unfold revealing itself as the means to adapt the connectivity and information to the users needs and preferences in a transparent way.

The evaluation of the users' options, needs, preferences and choices as well as the environment that surrounds them allows the logic characterization of its context. Through context analysis of a user it becames possible to infer about some of his habits, predict usability changes and to take automatic decisions about some matters, like connectivity, applications's usability change according to the its surroundings, personalizing and adapting the application's behavior to the users conditions. Sensor networks are valuable information sources as they provide additional information that usually mobile devices do not have. For this reason, sensor networks are considered one of the best information sources from the context analysis point of view.

In a heterogeneous network we can find different technologies of networking (i.e. WiFi, WiMAX, 3G, etc.) and one of the recurrent problems is to find a common feature that allows a continuous experience to the user. The 802.21 protocol is that common feature and though its main purpose is to address handover procedures, it operates in the second layer of communications and access information that belongs to the third one without actually making a connection to the third layer. In this dissertation we will demonstrate how to take advantage of this 2,5 layer to access and provide context information. The context transport based on 802.21 proposes itself to approach this next step through a proof of concept that encompasses a cooperation between the 802.21 protocol, context management platforms (information services) and sensor networks with the main goal of facilitating the personalization of applications and devices in a automatic and transparent way to the user.

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos e Siglas

2G/6G 2/6 vezes a força da gravidade (G)

3G Terceira geração de comunicações móveis

3GPP 3rd Generation Partnership Project

3GPP2 3rd Generation Partnership Project 2

AODV Ad hoc On-Demand Distance Vector

AP Access Point

API pplication Programming Interface

ARM Advanced RISC Machine

ATM Asynchronous Transfer Mode

CLDC Connected Limited Device Configuration

CPU Central Processing Unit

CSV Comma-separated values

CTP Collection Tree Protocol

CxB Context Broker

CxC Context Consumer

CxP Context Provier

DHCP Dynamic Host Configuration Protocol

ECC Elliptic curve cryptography

EEML Extended Environments Markup Language

GNU GNU's Not Unix

GPL General Public Licens

HNG Heterogeneous Networking Group

HTTP AHypertext Transfer Protocol

HTTPS AHypertext Transfer Protocol Secure

IANA Internet Assigned Numbers Authority

IDE Integrated Development Environment

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IM Instant Messaging

IO Input Output

IP Internet Protocol

IQ Info/Query

JID Jabber ID

JSON JavaScript Object Notation

L1 ou Camada 1 layer 1 (PHY)

L2 ou Camada 2 layer 2 (MAC and/or LLC)

L3 ou Camada 3 layer 3 (Network Layer)

LAN local area network

LLC Logical Link Control

LQRP Link Quality Routing Protocol

MAC Media Access Control

MDIP Mobile Information Device Profile

MICS Media Independent Command Service

MIES Media Independent Event Service

MIH Media Independent Handover

MIHF Media Independent Handover Function

MIH SAP Media Independent Handover Service Access Point

MIIS Media Independent Information Service

MIPS Microprocessor without interlocked pipeline stages

MN Mobile Node

ODTONE Open Dot Twenty ONE

OSI Open Systems Interconnection

PDA Personal Digital Assistant

PHY Physical Layer

PoA Point of Attachment

PoS Point of Service

PT Portugal Telecom

PubSub Publish Subscribe

RAM Random Access Memory

RDF resource description framework

RSS Really Simple Syndication

SAP Service Access Point

SCTP Stream Control Transmission Protocol

SASL Simple Authentication and Security Layer

SMS Short Message Service

TCP Transmission Control Protocol

TLS Transport Layer Security

TLV Type Length Value

UDP User Datagram Protocol

UMTS Universal Mobile Telecommunication System

URL User Datagram Protocol

XEP XMPP Extension Protocols

WiFi Wireless Fidelity

WiMAX Worldwide Interoperability for Microwave Access/Interoperabilidade Mundial para Acesso de Micro-ondas

WLAN Wireless Local Area Network

XML Extensible Markup Language

XMPP Extensible Messaging and Presence Protocol

Definições

802.11 Norma que descreve o funcionamento de uma rede local sem fios WiFi.

802.15.4 Norma que especifica interacção ao nível da camada física e MAC para comunicação sem fio de baixo débito.

802.16 Norma que descreve o funcionamento de uma rede metropolitana sem fios.

802.21 Norma que suporta mecanismos e procedimentos que facilitam um handover entre duas redes.

Adaptacao Capacidade de um software ou hardware em optimizar o seu funcionamento em função das condições a que está sujeito.

Ad hoc Em redes de computadores, denomina um tipo de rede que não possui um nó central e onde todos os nós encaminham as comunicações que provêm dos nós vizinhos.

Atom Formato de dados, baseado em XML e metadados, utilizado para distribuição de conteúdos.

Beacon Frames Tipo de gestão de frames utilizado em WLANs de IEEE 802.11. Contém toda a informação sobre uma reed e é transmitida periodicamente para anunciar a presença de uma rede WLAN.

Bluetooth Protocolo padrão de comunicação sem fio de baixo alcance e baixo consumo.

Broadcast Processo através do qual é transmitida informação para muitos receptores ao mesmo tempo.

Camada/Layer Subdivisão de um sistema do ponto de vista das comunicações.

Celula Área geográfica coberta por um transmissor/receptor.

Chat Conversação através de mensagens instantâneas.

Child Node Tipo de nó XML que deriva de um um outro nó na estrutura em árvore da informação.

Collection Node Tipo de nó XMPP. O Collection node agrega em si informação de Leaf Nodes.

Context Consumer (CxC) Entidade de uma rede que obtém informação de contexto gerada por um context provider e disponibilizada por um context broker.

Context Broker (CxB) Entidade de uma rede que disponibiliza informação de contexto.

Context Provider (CxP) Entidade de uma rede que informação de contexto que será disponibilizada por um context broker.

Data Link Layer Camada de ligação pertencente ao modelo OSI, também conhecida como camada 2 ou L2, responsável pela transferência de dados entre nós de rede adjacentes.

Dynamic Host Configuration Protoco (DHCP) Protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais através da atribuição de endereços IP.

Escalabilidade Característica que indica a capacidade de um sistema em lidar com um possível aumento de elementos ou carga de processamento.

Ethernet Tecnologia de ligação por cabo para redes locais.

Feed Formato de dados usado em formas de transmissão de dados, tipicamente utilizado por web sites ou blogs.

Fetch Processo de obtenção de dados

Flooding Disseminação exacerbada de informação pelos nós de uma rede.

Framework Abstracção que une códigos comuns entre vários projectos de software providenciando uma funcionalidade genérica.

Gateway Equipamento intermediário que pode interligar redes, domínios e traduzir protocolos.

Geo Tracking Descoberta da localização através de IP.

Google Maps Serviço disponibilizado pela Google, que permite a localização geográfica através de uma interface gráfica de interacção com um mapa mundo.

Handover Processo pelo qual um nó móvel preserva o fluxo de tráfego após ocorrer uma transição na ligação.

Hardware Conjunto de componentes electrónicos em comunicação que compõe os equipamentos/dispositivos electrónicos (e.g. Computadores, portáteis, telemóveis).

Heterogeneidade Característica que define a composição de um sistema por elementos diferentes.

Information Elements São tipos de estruturas de dados utilizados para a troca de informação.

Info/Query (IQ) Tipo de pacote utilizado pelo protocolo XMPP para obter e definir informação no servidor.

Interoperabilidade Capacidade de inter-comunicação entre sistemas.

Jabber Conjunto de protocolos XML que permite a troca de mensagens instantâneas.

Jabber ID Identificação única de cada utilizador relativa ao protocolo XMPP.

Java Equipamento intermediário que pode interligar redes, domínios e traduzir protocolos.

Jive Companhia de desenvolvimento de software orientado a redes sociais, software de colaboração e software comunitário.

Leaf Node TIpo de nó XMPP. O Leaf node é um nó terminal onde a informação é disponibilizada e não pode agregar em si outros nós.

Mashup Website ou aplicação que utiliza conteúdo de várias fontes para fornecer um serviço.

Many-to-many Tipo de relação entre entidades. Descreve uma relacção de várias entidades para várias entidades.

Media Independent Handover Processo de handover entre redes de comunicação que não depende do meio/tecnologia de comunicação utilizada.

Mesh Network Tipo de rede onde cada nó da rede pode funcionar como um router independentemente de estar conectado a outra rede ou não.

Middleware Elemento que faz a mediação entre softwares. Transporta informação e dados entre programas que utilizem diferentes protocolos de comunicação, plataformas e dependências do sistema operativo.

media independent handover function (MIHF) Componente que implementa e disponibiliza serviços MIH.

MIH User Utilizador de serviços MIH.

Mobile Node (MN) Nó de rede com capacidades móveis.

Mobile IP Protocolo de comunicações desenvolvido para possibilitar que os dispositivos se movam entre redes mantendo um endereço IP permanente.

Mobilidade Capacidade de movimento.

Multi-party Serviços que permitem que dois ou mais utilizadores usem o mesmo recurso.

Namespace Identificador abstracto que atribui contexto a um item

Netbeans IDE de desenvolvimento de software multi-linguagem.

Network Layer Camada de rede pertencente ao modelo OSI, também conhecida como camada 3 ou L3, responsável pelo encaminhamento entre a origem e o destino incluindo o encaminhamento através de elementos intermediários.

No de Sensores Nó de uma rede, geralmente sem fio, equipado com um ou mais sensores.

Openfire Equipamento intermediário que pode interligar redes, domínios e traduzir protocolos.

Overhead Processamento, armazenamento ou transmissão em excesso.

Overlap Situação em que duas redes sem fios possuem cobertura de sinal simultânea numa localização geográfica.

Pachube Web Site de agregação de informação de contexto.

Parsing Processo que analiza padrões numa sequência de dados extraindo informação relevante.

Payload Também denominado como carga útil, refere-se aos dados reais transmitidos por um pacote (excluindo o cabeçalho e informação de sinalização).

Peer-to-peer Tipo de arquitectura de sistemas distribuídos caracterizada pela descentralização das funções na rede. Cada nó é, simultaneamente, servidor e cliente.

Presence Tipo de informação de um utilizador no protocolo XMPP.

Request Tipo de mensagem que geralmente sinaliza um pedido.

Response Mensagem gerada em resposta a uma mensagem do tipo Request.

Rooms Sala virtual onde vários utilizadores trocam mensagens instantâneas.

Runtime Identifica uma instalação de um dado software num computador.

Schema Forma como a informação é estruturada numa mensagem.

Service providers Entidade que providencia serviços a outras entidades.

Shared Secret Metodo de criptografia onde um pedaço de dados apenas é conhecido por elementos envolvidos numa transmissão segura.

Smack Biblioteca Java de clientesXMPP.

Software Sequência de instruções que são executadas por um computador implementando uma sequência de operações lógicas com vista à manipulação de informação para um objectivo específico.

Stack Protocolar Conjunto de protocolos utilizado numa rede de comunicações. A *stack* protocolar é estruturada numa hierarquia de camadas. Encontra-se em cada cliente e servidor e a utilização desta estrutura permite a utilização de vários protocolos consoante a arqutectura da rede.

Stanza Unidade discreta de informação estruturada enviada entre dois utilizadores através de um stream XML.

Stream Fluxo de dados,

Testbed Plataforma experimental para o desenvolvimento de projectos.

Tinder Bibilioteca Java de componentes XMPP.

Topologia Forma através da qual os elementos de uma rede estão dispostos.

Trama Composição de todos os dados de uma mensagem transmitida entre duas entidades.

Transceiver Dispositivo electrónico que opera como transmissor e receptor de sinal.

Trigger Mecanismo de software que despoleta uma acção quando é ultrapassado um limiar de operação pre-definido.

Transicao Processo pelo qual um nó móvel altera a ligação que o conecta à rede. Alterar uma ligação implica mudança do ponto de ligação.

Ubiquidade Característica de algo que se encontra em todos os lugares.

Web Service Serviço remoto utilizado invocado através de uma rede.

Wireless Definição de um meio sem fio de comunicação numa rede.

Wireless carriers Operador de redes que envolvem comunicações sem fio.

Whack Biblioteca Java de componentes XMPP.

XMPP Core Memorando da Jabber Software Foundation que define características núcleo do protocolo XMPP.

Capítulo 1

Introdução

A evolução das redes heterogéneas face ao mundo que nos rodeia criou uma dependência a quase todos os nveis da sociedade. Já não se coloca a questão de ter ou não conectividade, neste ou naquele lugar, ou mesmo, se existem serviços disponíveis para o efeito, mas sim, que tipo de conectividade e que tipos de serviços. Esta questão pode ser reduzida de "ter ou não"para "quanto se tem".

A norma *IEEE* 802.21 [1] vem fornecer meios e ferramentas para ultrapassar o problema de falta de conectividade criada pela transição entre meios de ligação diferentes ou simplesmente entre áreas de cobertura adjacentes. Esta norma permite a sua utilização ao nível da camada L2 mas com acesso a um determinado tipo de informação que normalmente só se encontra acessível pela camada L3. Esta particularidade virtualiza uma camada L2,5 que permite uma nova exploração da rede do ponto de vista de contexto. Através desta norma é possível eliminar a questão de "ter ou não"ligação na transição entre dois locais de acesso e permite um maior foco na questão "quanto se tem".

As redes de comunicação actuais são compostas por equipamentos da mais diversa natureza, em que cada equipamento gera e utiliza informação ainda mais diversificada. As plataformas de gestão de contexto, apresentam uma forma de agregar, gerir e disponibilizar essa informação numa forma lógica e acessível, fomentando serviços, mecanismos e funcionalidades do mais variado possível que permitem a utilização desse tipo de dados à posteriori. Através das plataformas de gestão de contexto consegue-se caracterizar o ambiente de funcionamento dos equipamentos, suas necessidades e requisitos em comunhão com os restantes elementos da rede e serviços subjacentes.

No entanto, a informação gerada pelos equipamentos de uma rede não é, muitas vezes, suficiente para caracterizar um contexto de utilização, para esse efeito, recorre-se a redes de sensores. As redes de sensores trazem uma melhoria na qualidade e quantidade de informação sobre o contexto físico que rodeia os utilizadores, contribuindo para um enriquecimento das plataformas de gestão de contexto.

Embora estas tecnologias e abordagens já estejam disponíveis há algum tempo, existem questões pertinentes como a integração das mesmas tirando vantagens de todos os seus benefícios e particularidades. A dissociação destas áreas tecnológicas introduz alguns proble-

mas como por exemplo, o facto de os procedimentos de *handover* carecerem de informação específica referente ao contexto em que um utilizador se encontra, seja do ponto de vista dos requisitos físicos, preferências aplicacionais ou estado do ambiente envolvente. Outro problema que se pode colocar, na mesma linha de raciocínio, é a falta de informação que permita às aplicações, ajustar as suas funcionalidades ao contexto do utilizador, adaptar os conteúdos às preferências dos utilizadores e personalizar os dispositivos consoante a utilização e ambiente envolvente. Este é o problema que a dissertação se propõe a abordar criando uma estrutura que, através de uma camada de inteligência constantemente renovada pela informação de contexto, forneça aos utilizadores e serviços, meios e mecanismos para melhorar a utilização e gestão da rede.

1.1 Aplicações Práticas

Actualmente, os dispositivos possuem capacidades tecnológicas que permitem a utilização de múltiplas interfaces para descobrir e interpretar o contexto que rodeia e envolve o utilizador. Através desta interligação de dados é possível extrapolar as necessidades, requisitos e preferências do utilizador e, com esta informação, adaptar, não só a utilização e o funcionamento do equipamento ao seu contexto como a resposta da rede aos pedidos que lhe são efectuados. [2]

1.1.1 Handover em Transportes Públicos

Nos transportes públicos da actualidade, a conectividade com a rede depende grandemente da capacidade e interfaces disponíveis no equipamento do utilizador e encontra-se pouco integrada com o contexto móvel inerente ao meio de transporte.

Um cenário de uso generalizado tem os seguintes contornos: o utilizador encontra-se dentro de um comboio (e.g.) e está a aceder à internet através da sua ligação 3G, quando o comboio chega à estação e o utilizador abandona a carruagem, tipicamente o acesso à internet mantém-se através da ligação 3G.

Na nossa visão, o cenário de uso mantém-se semelhante, mas a experiência de utilização é transparentemente alterada para benefício do utilizador. O utilizador, enquanto em movimento, acede à internet através da sua ligação 3G. No entanto, ao chegar a uma estação, entram em funcionamento dois mecanismos: o primeiro, auxiliado por sensores embutidos, infere sobre o movimento do utilizador e conclui que o comboio está parado; o segundo, além de o utilizador estar conectado por 3G, a sua interface sem fios faz um pesquisa de redes disponíveis. Se o resultado dos sensores indicar que o veículo está parado e a pesquisa detectar uma rede sem fio de uma estação, é efectuado um *handover* para o AP da estação sem interromper a experiência do utilizador.

Esta abordagem apresenta vantagens inquestionáveis a vários níveis. Em termos de velocidade, o utilizador passa a usufruir de uma interface cuja tecnologia permite a utilização de taxas de transmissão de dados a uma velocidade superior. O custo de navegação é reduzido substancialmente, uma vez que o custo por dados na utilização de uma ligação 3G é bastante

mais elevado que a utilização de uma tecnologia WiFi ou WiMAX. Por fim, o utilizador beneficia destes dois melhoramentos na sua experiência de uma forma totalmente transparente para a sua experiência móvel. De facto, a única alteração imediata que o utilizador deverá visualizar será o aumento da rapidez de obtenção de conteúdos.

1.1.2 Difusão de Informação em Centros Comerciais

Os centros comerciais são lugares onde se concentra um grande número de pessoas, e, ao longo do seu período de funcionamento o fluxo de indivíduos que por ele passam é considerável. Este tipo de instalação comercial tem apenas um objectivo: vender. Para este efeito nada melhor que aproveitar a grande quantidade de pessoas que por lá passam ao mesmo tempo que se tira partido das suas necessidades consumistas com publicidades personalizadas distribuídas directamente para os equipamentos móveis.

Um exemplo de um cenário recorrente pode ser descrito da seguinte forma: o Luís vai a um centro comercial Y, para passear e fazer algumas compras. Enquadrando neste cenário os conceitos propostos ao entrar no centro comercial Y e mediante as suas escolhas pessoais especificadas pelas suas redes sociais, a rede do centro comercial infere os seus gostos e envia mensagens com os produtos que calculou serem os mais atractivos para este cliente com o formato "Produto A na loja B a C euros". Imediatamente, se o utilizador tiver especificado que procura roupa na categoria de roupa de Inverno, recebe uma mensagem dizendo "Produto Casaco na loja B a C euros". É possível ainda, através do sensor de movimento ser detectado se o utilizador está com pressa ou se se encontra simplesmente a passear pelo centro comercial obtendo simultaneamente a localização do utilizador em relação à loja. Agregando esta informação e fornecendo-a à rede, ao passar pelas lojas, em "modo de passeio", pode ir recebendo no seu equipamento móvel as promoções e produtos mais atractivos na loja mais próxima de si, por outro lado, se se encontra em "modo visita rápida"apenas são demonstrados os produtos previamente definidos como interessantes.

A inclusão da visão apresentada neste cenário amplia a possibilidade de negócio nas instalações comerciais através do marketing e publicidade orientados ao utilizador e às suas necessidades de consumo. Com efeito, obtém-se benefícios directos e visíveis tanto para o utilizador do equipamento móvel como para as lojas que se encontram nos centros comerciais. O utilizador possui a vantagem de os conteúdos serem seleccionados convenientemente para si, pelo que procura, pelo que gosta e pela sua disponibilidade de tempo num centro comercial. As lojas beneficiam claramente deste serviço uma vez que os seus produtos são anunciados e publicitados aos clientes sem que estes tenham de entrar na loja ou ler panfletos de publicidade.

1.1.3 Controlo generalizado de Emergências

Em situações de emergência (e.g. incêndios, terramotos, *etc.*) em locais públicos de grande escala é essencial que os elementos das equipas de socorro, sejam bombeiros, polícia ou paramédicos, mantenham capacidade de ligação constante e as suas necessidades a esse nível sejam tratadas com prioridade em detrimento dos outros indivíduos que se encontram no local que devem ser aconselhados, tendo em conta a situação, nos procedimentos a tomarem para sua segurança.

Numa situação não prevista de emergência, as pessoas tentam sair das instalações/locais publicas da forma mais rápida, desordenadamente e por zonas não recomendadas. Além deste problema, existe o congestionamento causada pelo rápido aumento no volume de comunicações num único local, criado pelas pessoas a tentarem desesperadamente contactar com alguém próximo. Esta situação dificulta a comunicação entre as equipas de socorro reduzindo a rapidez e eficácia dos processos de salvamento.

Como forma de gerir estas situações da melhor maneira possível, a detecção destes eventos pode ser efectuada por sensores das mais variadas formas, através de hardware por sensores (e.g. sensores de fumo, vibração, som, etc.) e através de software por controlo do fluxo das chamadas de um dado local. Após a detecção de situações de emergência podem ser localizadas as pessoas existentes no local através dos seus equipamentos móveis e iniciar as medidas de controlo. As medidas de controlo passam pelo envio, de mensagens com imagens com os planos para a saída do local mais segura, envio de mensagens com conselhos e procedimentos de segurança e monitorização da localização destes indivíduos para que, se eventualmente, alguém estiver preso ou incapacitado seja facilmente localizado pelas equipas de socorro. Quanto à ligação, deve ser atribuído aos elementos das equipas de socorro um estatuto de prioridade superior no acesso aos meios de comunicação para que tenham sempre disponíveis formas de contacto entre si e entre o mundo externo.

A implementação deste sistema pode tornar-se uma mais valia no auxílio e contenção de emergências orientando as pessoas através do seu equipamento móvel e permitindo aos elementos das equipas de socorro possuir uma prioridade superior para, em casos de necessidade, estarem sempre contactáveis uma vez que são as entidades fulcrais das operações de salvamento.

1.2 Enquadramento

Esta dissertação surge da confluência de três áreas tecnológicas, redes heterogéneas, redes de sensores e gestão de contexto. As redes heterogéneas são indubitavelmente a pedra angular desta dissertação, actuando como suporte e ligação entre as redes de sensores e a gestão de contexto. As redes de sensores fornecem diferentes tipos de informação que, através das redes heterogéneas, são transportados para entidades que processam todos estes dados permitindo a sua disponibilização. Este tipo de organização permite a integração das três áreas tecnológicas duma forma perfeitamente orgânica e distribuída.

O tema desta dissertação surge de uma sinergia criada entre o projecto ODTONE (ver Anexo A.1), relacionado com as redes heterogéneas e o projecto PT Context Broker (ver Anexo C), relacionado com a gestão de contexto, ambos em desenvolvimento no Instituto de Telecomunicações de Aveiro.

1.3 Objectivos

Esta dissertação tem como principal objectivo apresentar uma arquitectura e a implementação de um protótipo, que à semelhança da sua designação, permita incrementar a sinalização 802.21 com capacidades de contexto. Pretende-se demonstrar, como o protocolo 802.21 pode ser extendido a novos domínios e como podem ser aproveitadas as suas funcionalidades e mecanismos, para, em conjunção com uma plataforma de gestão de contexto, baseada no protocolo XMPP, permitir uma personalização e adaptação de conteúdos, dispositivos e aplicações ao contexto de utilização.

O foco da dissertação não se centra na capacidade de *handover* do protótipo, mas antes no uso da camada L2,5 em que opera o protocolo IEEE 802.21 possibilitando a extracção de informação de contexto impulsionando múltiplos serviços e funcionalidades de utilização personalizada.

1.4 Organização

A dissertação está estruturada em sete capítulos, introdução, estado de arte, arquitectura, implementação, avaliação do protótipo e conclusões.
A **Introdução** é composta por uma breve apresentação e descrição dos elementos que potenciaram esta dissertação face ao mundo real, seguida do enquadramento onde é descrito em que âmbitos se enquadra a dissertação nas várias áreas tecnológicas, os objectivos a que se propõe e a organização estrutural do documento.
O **Estado de arte** apresenta avanços científicos, problemas e soluções encontradas nas várias áreas que compõe e suportam esta dissertação. São também apresentadas tecnologias e projectos em que a arquitectura é baseada e nas quais a implementação do protótipo foi desenvolvida.
A **Arquitectura** é o capitulo onde é apresentada a proposta de arquitectura como solução conceptual para o problema enunciado.
A **Implementação** descreve o protótipo implementado como prova de conceito validando a arquitectura proposta.
Na **Avaliação do Protótipo** apresentam-se os resultados obtidos e extrapolados pela prova de conceito e respectivos cenários.
Nas **Conclusões** finaliza-se a dissertação, demonstrando algumas aplicações práticas e sugestões para trabalho futuro que derive desta dissertação.

Capítulo 2

Estado de Arte

Apresentam-se alguns temas e tecnologias que impulsionam toda a visão desta dissertação, nomeadamente, as tendências tecnológicas, as redes heterogéneas, as redes de sensores, a gestão de contexto, a norma IEEE 802.21 e o protocolo XMPP.

2.1 Tendências Tecnológicas

O transporte de contexto baseado em 802.21 é uma abordagem inovadora à integração das três áreas tecnológicas que já se circundam numa lenta aproximação há algum tempo, as redes heterogéneas, as redes de sensores e a gestão de informação de contexto.

Apresentam-se alguns temas, tecnologicamente específicos, que impulsionam e sustentam o transporte de contexto baseado em 802.21 tanto ao nível prático como teórico.

2.1.1 Redes de Sensores Cientes de Contexto

As redes de sensores apresentam algumas questões sensíveis em vários aspectos que advêm da sua natureza, como a escalabilidadade, gestão energética, acesso aos dados, segurança e privacidade.

A utilização de sensores nas redes de comunicação centra-se na análise de padrões baseados em medidas e valores recolhidos, do contexto onde se encontram. Estas análises são enviadas à posteriori para a rede com vista ao auxílio na gestão de energia, acesso a serviços e performance da própria rede.

Até há algum tempo a existência de sensores cujas medidas influenciem o ajuste de condições num determinado contexto obrigava à intervenção humana para leitura e controlo do equipamento. Além disso, a falha na gestão energética pode levar os sensores que dependem de baterias a serem vigiados constantemente e a necessitarem de manutenção regular. Neste sentido, as redes sem fios de sensores permitem uma integração destes dispositivos nas respectivas redes capacitando a obtenção de dados de forma contínua e permitindo uma monitorização remota. A recolha de dados automática motiva o interesse na utilização de redes de sensores integradas nas redes de comunicação utilizadas no dia a dia. Embora apresentem bastantes vantagens, esta integração revela algumas preocupações ao nível da robustez, privacidade e segurança de informação [3].

Para resolver estas questões, a solução passa pela criação de uma plataforma de gestão de contexto e sensores, bem como a adopção de algumas regras de funcionamento para os próprios dispositivos [3].
Os sensores reportam periodicamente o seu estado de funcionamento e o nível de bateria do dispositivo. Este mecanismo dispensa uma constante vigilância humana e permite que se controle periodicamente o seu estado remotamente.
Os dados recolhidos pelos sensores são enviados com uma periodicidade diferente baseando-se na sua função. De uma forma geral, sensores de temperatura não necessitam de enviar o seu estado ao mesmo ritmo que um sensor de aceleração. Tipicamente os sensores não necessitam de estar continuamente a recolher dados. Esta característica permite que o equipamento desligue alguns sistemas durante os momentos nos quais se sabe à partida que não afectarão a performance do sistema. Estas medidas permitem uma gestão energética bastante eficaz, uma vez que os sensores só irão consumir energia quando necessitarem de efectuar uma operação.
Quanto a questões de privacidade e segurança, a solução passa pela implementação um sistema de permissões e accounting que controla o acesso aos serviços disponibilizados pela plataforma de gestão.

Uma solução encontrada permite o acesso a informação de contexto relativo a redes de sensores adaptando os equipamentos ao contexto em que se encontram e, regulando o comportamento dos dispositivos mediante a sua utilização, obtém uma optimização na gestão energética, no controlo de privacidade e segurança e permite a monitorização dos sensores na rede remotamente. Desta forma é possível uma extensão destas redes e do seu suporte a diferentes contextos, interfaces e políticas de gestão [3].

2.1.2 Handover facilitado por Informação de Contexto

O crescente mercado de dispositivos móveis (e.g. PDAs, *Smartphones, Netbooks, Laptops, etc.*) aliado à evolução dos meios de comunicação indica a necessidade da existência de serviços orientados à mobilidade. A mobilidade, por sua vez, implica serviços que se adaptem às alterações de contexto. Devido à existência de vários meios de acesso à rede (e.g. WiFi, WiMAX, 3G , Bluetooth, *etc.*) cada tecnologia tem as suas vantagens pelo que é necessário considerar o *handover* baseado nas condições de contexto do equipamento e/ou utilizador.
A heterogeneidade das redes e dos elementos que as compõe complica as condições para a conjugação de informação de contextos diferentes e *handover* entre interfaces e meios tecnologicamente diferentes [4].

Os dispositivos móveis encontram-se, cada vez mais, equipados com múltiplas interfaces de comunicação. Tendo em conta esta particularidade, faz sentido que os serviços utilizados pelos equipamentos tenham conhecimento das capacidades de cada interface assim como do contexto em que se encontram.
Existem algumas considerações a ter em conta no recurso ao procedimento de *handover*, como por exemplo, a largura de banda, a cobertura ou custo por transferência de dados. Quanto ao contexto, os serviços devem ser capazes de localizar o utilizador por forma a disponibilizar conteúdos adaptados à sua localização. As condições de contexto e *handover* apresentados requerem que os serviços aplicacionais se mantenham cientes do que os rodeia, do estado em que se encontram, dos serviços consumidos, e das necessidades ao nível de rede que apresentam.

Tendo em conta os suportes tecnológicos e os problemas apresentados, uma solução baseia-se na criação de uma arquitectura *middleware* para serviços [4]. A solução baseada em *middleware* permite o desenvolvimento de serviços conscientes do contexto em que se encontram. A arquitectura sugerida em [4] oferece um conjunto de mecanismos para gestão de *handovers* baseados em contexto de forma tecnologicamente transparente. Esta solução baseia-se na criação de uma arquitectura com três camadas, serviços, capacidades e mecanismos. A camada de serviços é composta por um modelo de serviços baseados na mobilidade do dispositivo que utiliza a camada de capacidades para reconhecer e gerir situações de mobilidade e gestão de capacidades específicas para cada domínio. A camada de mecanismos encapsula as interfaces com as várias tecnologias ao nível de contexto e detecção de *handovers*.

Com esta solução é possível desenvolver serviços cientes de contexto em redes heterogéneas tendo em vista a gestão dos procedimentos de *handover* nos meios de comunicação. É possível ainda suportar capacidades específicas para cada domínio e tecnologia através da estratificação da arquitectura nas camadas referidas [4].

2.1.3 Serviços Sensíveis ao Contexto

A evolução dos componentes electrónicos contribuíu bastante para o aumento dos recursos computacionais disponíveis assim como para a diversificação dos meios de comunicação. A riqueza de recursos e dos equipamentos não se traduz em utilidade em todos os cenários. Para que exista comunicação entre elementos computacionais heterogéneos ou entre redes heterogéneas é preciso um elemento intermédio que entenda ambos meios de comunicação que muitas vezes é o ser humano. Torna-se, portanto, crítico encontrar um meio através do qual os vários dispositivos e vários meios de comunicação possam interagir sem necessitar da intervenção do utilizador.
Uma perspectiva orientada a serviços simplifica o problema traduzindo os vários recursos na forma de serviços. Por exemplo, um dispositivo móvel deixa de ter de reconhecer uma impressora pelo que é e pela tecnologia que a acompanha e passa a identifica-la como um serviço de impressão generalizado. Os serviços adaptam-se de forma dinâmica consoante a mobilidade do utilizador e o contexto que o rodeia [5].

Uma solução para este problema pode ser encontra através da utilização de uma *framework* de disponibilização de serviços baseada em três módulos, computação ciente de contexto, aquisição de informação de contexto e distribuição de contexto [5].
A computação ciente de contexto permite aos utilizadores obter uma experiência computacional direccionada ao seu contexto actual. Se o utilizador se mover rapidamente, de carro ou comboio, faz sentido que o dispositivo móvel lhe disponha informação sobre o estado do tráfego na sua trajectória ou apresente o tempo de atraso do comboio. Noutras situações, como uma reunião, mediante o som recebido pelo microfone do dispositivo móvel pode adaptar o seu som de toque caso receba uma chamada.
A aquisição de informação de contexto pode ser obtida através de sensores. No entanto, a aquisição de dados sensoriais só faz sentido se estes puderem ser correlacionados com as actividades do utilizador. Isto é conseguido através de uma camada de inteligência que utiliza informação de sensores para ajudar na tomada de decisões.
Finalmente, a distribuição de contexto, é através deste modelo que os serviços tomam conhe-

cimento das condições de contexto em localizações remotas. Esta funcionalidade é importante principalmente em tecnologias de grande área de alcance como o WiMAX e o 3G, onde existe a possibilidade da existência de contextos que possam interessar ao serviço do utilizador que não se encontrem nas imediações mas podem ser transportados através do mecanismo de disponibilização de contexto.

Por fim, a conjunção dos elementos referenciados permite a implementação de uma *framework* para a construção de serviços que se adaptem ao seu contexto, fornecendo ao utilizador serviços personalizados e indicados para as suas necessidades. Uma forma de resolver esta lacuna pode ser conseguida fornecendo informação sobre as redes de acesso, serviços locais e informação sobre o respectivo contexto [5].

2.1.4 Serviços de Informação baseados em 802.21

As tecnologias de acesso ao meio têm vindo a diversificar-se (e.g. UMTS, WLAN, WiMAX, *etc.*) e não existe um consenso quanto ao meio global de acesso. A heterogeneidade das redes tende a aumentar.
Em conjunção com as redes heterogéneas, a mobilidade implica alterações constantes entre redes de acesso e isso implica *handovers* baseados em decisões necessariamente mais exactas. As condições que implicam a mudança de rede necessitam de ser avaliadas e controladas. O controlo pode ser implementado através da adaptação dos sistemas ao contexto ambiental, aplicacional e de serviços, minimizando a intervenção humana.
Para que a adaptação às alterações seja bem sucedida é necessário que as entidades sejam abastecidas com informação relevante acerca do seu contexto, incluindo informação sobre as redes a que se interligam [6].

Para responder as estas necessidades é possível implementar um serviço de informação baseado em 802.21 que forneça os dados necessários [6]. Esta solução implica o desenvolvimento das três componentes baseadas na norma 802.21, mas orientados à informação de contexto, um serviço de informação, um serviço de eventos e um serviço de comandos.
Com estes elementos é possível implementar uma arquitectura orientada a contexto dividida em três camadas, a camada de serviços, a camada de convergência e a camada de sensores. A camada de serviços implica a interacção com os serviços e aplicações que vão obter proveito desta solução. A camada de convergência encapsula as plataformas de gestão de contexto, a forma como a informação é obtida e armazenada para disponibilização posterior. A camada de sensores define os dados obtidos por sensores embutidos na rede e por dispositivos sensoriais independentes que possam vir a fornecer dados relevantes [6].

Esta solução permite a criação de uma arquitectura que suporta uma utilização tradicional das redes de acesso onde não é necessário um conhecimento do contexto envolvente bem como abordagens mais evoluídas, com serviços que requerem conhecimento de contexto para tomar decisões de *handover*. Os aspectos da arquitectura apresentados permitem integrar a informação de contexto com os mecanismos de *handover* criando uma camada de inteligência na avaliação das condições de uma rede em detrimento de outras.
Estes mecanismos permitem auto-adaptação, significando menor necessidade para a intervenção humana e melhoramento na experiência de utilização [6].

2.2 Redes Heterogéneas

Uma rede heterogénea é uma rede que, na sua composição, integra elementos de tecnologias, natureza, funcionalidades e mecanismos diferentes. A ligação e operação neste tipo de redes são conseguidos através de interacção entre protocolos e sistemas operativos diferentes.

Um dos objectivos fundamentais das redes heterogéneas, e em foco nesta dissertação, é a interoperabilidade. A **interoperabilidade** é a propriedade que permite a cooperação entre elementos com sistemas operativos diferentes de forma transparente através de protocolos suportados. A figura 2.1 exemplifica uma rede heterogénea e a sua interoperabilidade.

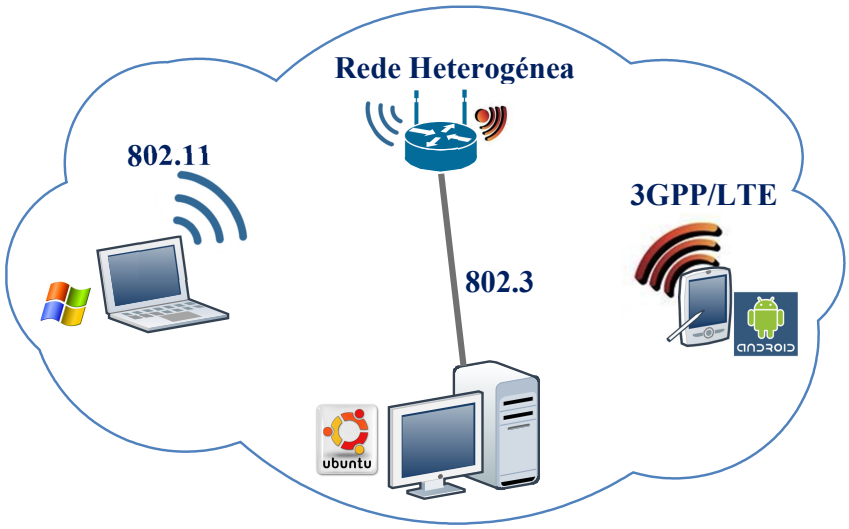


Figura 2.1: Rede Heterogénea

2.2.1 Diversidade e Robustez

As redes heterogéneas não padecem do problema de fragilidade intrínseco às redes homogéneas. Este problema tem a ver com os ataques aos elementos da rede, se uma rede for homogénea, as fraquezas desta rede serão generalizadas e comuns, aumentando a probabilidade de sucesso no ataque. Por contraste, numa rede onde as funcionalidades criticas são providenciadas por protocolos e implementações diversas, os ataques não conseguem obter um foco tão grande nem conseguem com apenas um ataque fazer desabar a infraestrutura completa da rede [7].

2.2.2 Ubiquidade

As redes heterogéneas beneficiam da utilização de redes sem fio nas mais diversas utilizações e locais. Uma vez que a ligação constante é uma realidade e a necessidade dos utilizadores por informação revela-se cada vez maior, verifica-se que existem redes sem fios em todos os contextos. As várias tecnologias utilizadas (e.g., WiFi, WiMAX, 3G, *etc.*) para a criação destas redes sem fios e a sobreposição das mesmas cria uma rede heterogénea que,

do ponto de vista do utilizador, é ubíqua aos vários ambientes em que se desloca possuindo, no entanto, características de utilização (e.g. velocidade, largura de banda, *etc.*) diferentes. Para o utilizador, embora algumas características de utilização possam vir a ser percepcionadas como diferentes, o *handover* entre as redes não o é. Esta característica é bastante importante em questões de integração, usabilidade e imersão por parte do utilizador [8].

Integração

Ao longo de um percurso descrito pelo movimento de um utilizador tornar-se-á inevitável a descoberta de redes sem fios em *overlap*, muitas vezes com tecnologias diferentes. Estas redes vão encontrando-se em contextos diferentes, seja uma rede pertencente a um centro comercial, a um hospital, a uma rede de transportes ou mesmo uma rede residencial. Tal como é facilmente perceptível, redes de contextos e tecnologias diferentes representam necessidades e características diferentes. É bastante importante seleccionar e separar as redes pelo seu contexto e capacidades para se poder fornecer ao utilizador, não só uma ligação mais adequada às suas necessidades, mas também considerando os custos associados a nível monetário e de recursos. Por exemplo, se um utilizador se encontra a fazer um *download* de um vídeo numa área apenas com cobertura 3G e o dispositivo identifica que o utilizador se está a movimentar, faz sentido que o *download* seja feito a uma velocidade reduzida, dando tempo para o utilizador se colocar numa zona com cobertura WiFi e aí sim aumentar a velocidade de download, uma vez que estará menos limitado pelos custos e velocidade da ligação. A questão da integração influencia a necessidade para estratificação dos vários tipos de redes, categorizando os tipos de ligação em camadas que podem mais facilmente ser escolhidas pelo dispositivo evitando que para cada rede recebida seja feito um estudo individualizado das capacidades da rede. Com a caracterização dos vários tipos de rede são evitados o dispêndio de recursos e tempo na avaliação das novas redes sobre as quais os utilizadores vão efectuando descobertas. [9]

Mobilidade

Como já referido, é expectável que um utilizador se movimente e, durante esse movimento, deseje manter a sua ligação. A mobilidade implica que exista algum mecanismo que proporcione ao utilizador uma experiência sem interrupções e sem necessidade de intervenção cada vez que for necessário reconexão ou conexão a uma nova rede. Para proporcionar uma imersão total, as redes heterogéneas recorrem muitas vezes ao procedimento de *handover*. Este procedimento envolve um mecanismo que efectua uma transição suave e transparente para o utilizador entre as duas redes e é essencial para um funcionamento correcto de uma aplicação numa rede heterogénea. [10]

2.2.3 Interligação de Utilizadores

Dado o tamanho da área que uma rede heterogénea pode ter, esta pode conter vários tipos de interligação entre os utilizadores. De entre estes tipos de interligação referem-se as duas principais, conexões celulares e conexões *ad hoc*. As redes celulares são redes hierarquicamente estruturadas e utilizadas para comunicações de longa distância, As ligações ad hoc são conexões *peer-to-peer* entre utilizadores, utilizadas para curta distância e não possuem uma hierarquia definida [10].

É possível agregar, numa rede heterogénea, os utilizadores e as entidades controladoras numa organização híbrida através da fusão das estruturas de redes celulares e redes ad hoc. Esta fusão cria um ambiente de intercooperação de utilizadores ao mesmo tempo que disponibiliza uma rede bem estruturada para comunicações de longa distância, gerindo os recursos disponíveis da melhor forma possível [10].

Organização topológica

Uma **estrutura de rede celular** é característica de redes onde existam vários operadores de comunicações. Esta estrutura apresenta uma organização estritamente hierárquica onde existe um nó *master* que corresponde à autoridade central. Existem entidades com poderes executivos que são geralmente *service providers* ou *wireless carriers* e competem mutuamente pelos utilizadores. Neste tipo de organização não são permitidas conexões *peer-to-peer* e são utilizadas ligações que implicam alto consumo energético [10].
Uma estrutura de rede **ad hoc** pode oferecer mais eficiência ao nível de gestão de recursos uma vez que permite a utilização de ligações sem fio de baixo consumo e baseia-se em ligações de cooperação *peer-to-peer* sugerindo uma abordagem aberta à organização. Esta estrutura não define uma hierarquia estrita e pode melhorar a experiência dos utilizadores quando a utilização depende grandemente de interacção entre recursos dos mesmos [10].

2.3 Redes de Sensores

Uma rede de sensores é, na sua essência, um conjunto de sensores que comunicam entre si criando uma rede de informação sensorial. Cada sensor pode ser visto como um componente de pequenas dimensões que combina a energia necessária para operação, poder de computação, comunicação sem fios e sensores específicos.

Com a evolução tecnológica pautada por um ritmo progressivo e estonteante, o conceito de sensor aproxima-se cada vez mais da premissa "mais em menos espaço". A tecnologia de sensores revela-se cada vez mais barata, com mais capacidade e menor tamanho. Estes factores contribuem para que as redes de sensores sejam cada vez mais comuns e com aplicações directas em áreas distintas.

2.3.1 Características

A posição dos nós de sensores não necessita de ser determinada à *priori*. Esta característica permite uma instalação em terrenos de difícil acesso. No entanto, para suportar esta fácil instalação é necessário que a rede de sensores possua uma capacidade auto-organizativa [11].

As redes de sensores possuem características distintas de um modelo particular de um sistema distribuído. Existem algumas limitações ao nível da utilização de recursos restritos de energia, ao nível da composição da topologia dinâmica de rede e ao nível da grande quantidade de nós que compõe uma rede de sensores. Tipicamente estas características fazem com que seja difícil a reutilização de algoritmos desenvolvidos para os casos mais gerais de sistemas distribuídos. Por este motivo, uma das soluções passa pela eleição de um "líder", um elemento que receba informação e faça a gestão dos restantes nós. Por outro lado existem soluções

que se concentram na atribuição individual, a cada nó, de um espaço de operação com o objectivo de combinar as informações individuais de cada sensor e monitorizar um fenómeno [12].

Entidades de uma Rede de Sensores

A acção numa rede de sensores pode ser caracterizada em três componentes, o sensor, o observador e o fenómeno [13].
O **sensor** é o componente físico responsável pela monitorização de um fenómeno reportando valores de medidas obtidas. Cada sensor é, por norma, composto por cinco componentes, o detector de hardware, memória, bateria, processador e transmissor-receptor.
O **observador** é o utilizador final que recebe os valores recolhidos pelos sensores e tem o poder de actuar sobre a rede. É comum, numa rede, a existência de vários observadores, pelo que, a acção permitida a cada um depende do tipo de gestão da rede.
O **fenómeno** é o alvo de interesse do observador, monitorizado pelo sensor. Geralmente uma rede de sensores pode monitorizar vários fenómenos simultaneamente.

Redes de Sensores e Redes *Ad Hoc*

Embora as redes de sensores possam ser encaradas como redes *ad hoc*, existem alguns pontos em que diferem conceptualmente. O número de nós numa rede de sensores é significativamente superior aos nós de uma rede *ad hoc*. Os nós de sensores são, por norma, instalados mais densamente e são tipicamente mais susceptíveis a falhas. A topologia de uma rede de sensores tende a variar com frequência dado o seu grau de mobilidade e fácil transporte devido ao seu tamanho, (geralmente, diminuto). As redes de sensores usam comunicações mais orientadas a *broadcast* enquanto que as redes *ad hoc* utilizam comunicações *peer-to-peer*. Os nós de sensores não possuem um tipo de identificação global uma vez que esta medida produziria uma grande quantidade de *overhead* causado pelo grande número de sensores que pode existir numa rede [11].

2.3.2 Caracterização de Contexto através de Sensores

Muitos dos dispositivos que são hoje utilizados já fornecem dados sensoriais (e.g. computadores portáteis, telemóveis, *etc.*). No entanto, estes dispositivos, não sendo orientados puramente à recolha de dados de sensores, não estão munidos fisicamente de sensores que monitorizem um grande número de fenómenos, pelo que a utilização apenas destes sensores numa rede não seria suficiente para caracterizar eficazmente um ambiente/contexto. A incorporação, nestes equipamentos móveis, de sensores que sejam capazes de satisfazer a necessidade de uma caracterização completa de um ambiente é altamente proibitiva do ponto de vista económico bem como do ponto de vista espacial. A sua utilidade para o utilizador detentor do equipamento nem sempre é essencial, pelo que o aumento do preço bem como o aumento de tamanho não seriam sempre desejáveis. Por este motivo, faz sentido incluir numa rede, pequenos componentes que se dediquem apenas à monitorização de fenómenos.

Esta abordagem permite uma redução de preços e uma diminuição do tamanho dos equipamentos móveis. Permitindo, simultaneamente, aumentar o número de nós melhorando o número de medidas, aumentar o número de fenómenos monitorizados, e melhorar o acesso dos equipamentos móveis a estes dados através da rede [11].

2.3.3 Utilizações

Os sensores, devido às suas características, podem ter múltiplas utilizações [12]. A utilização de redes de sensores conferem algumas vantagens na sua utilização. A diminuição do custo do sistema através da utilização comercial de tecnologias de rede (e.g. ATM, Ethernet, fibra óptica, *etc.*) em redes de sensores, e, aumentando ao mesmo tempo o desempenho. Podem também ser utilizados para monitorizar fenómenos em ambientes de difícil acesso nas várias áreas, militar, médica, geográfica, *etc.*, utilizando uma combinação de sensores de vários tipos. A redução de erros pode ser também conseguida através da combinação de sensores que recolhem informação com frequências diferentes.

2.3.4 Tipos de Sensores

As redes de sensores podem ser compostas por diferentes tipos de sensores, sísmicos, magnéticos, térmicos, visuais, infravermelhos, acústicos, radar, *etc.*. Esta variedade de sensores permite uma monitorização de um vasto número de fenómenos como a temperatura, humidade, movimento, luminosidade, pressão, níveis de ruído, detecção de certos objectos, *etc.*. [11].

2.3.5 Design das Redes de Sensores

O *design* de uma rede de sensores tem em consideração alguns factores que influenciam directamente o seu funcionamento, a tolerância a falhas, a escalabilidade, os custos, o contexto de operação, a topologia, as restrições de *hardware*, o meio de transmissão e o consumo energético [11].

Tolerância a falhas

Os nós das redes de sensores podem ter falhas, tanto ao nível de ligação como ao nível de *harware/software*, seja por falta de energia, danos físicos ou interferência ambiental. Por este motivo, a falha de um nó da rede não deve afectar o funcionamento geral da mesma. A tolerância a falhas é a capacidade que uma rede tem de manter o seu correcto funcionamento mesmo quando existem falhas por parte de alguns elementos que a compõe [11].

Escalabilidade

O número de sensores instalados para observar um fenómeno pode estar na ordem das centenas ou milhares. Dependendo da aplicação e do fenómeno em causa, pode ser necessário ascender esse número às centenas de milhares ou milhões. A questão de escalabilidade, resume-se, não só à capacidade que a rede tem para suportar essa variação no número de componentes mas também a forma como lida com o aumento da densidade de nós numa determinada área sem comprometer os seus objectivos [11].

Custos de Produção

Uma vez que uma rede de sensores pode ser composta por um grande número de nós, o custo individual de cada nó tem de ser ponderado tendo em conta o tamanho da rede de sensores. Em situações onde o custo de produção de um nó da rede de sensores faz resultar

um custo de produção exorbitante para compor uma rede de sensores, deve recorrer-se à instalação de sensores individuais de forma tradicional [11].

Contexto de Funcionamento

A instalação dos nós das redes de sensores é geralmente feita nas proximidades do fenómeno a ser observado. Por este motivo, o funcionamento pode variar dependendo do contexto em que se encontre, dentro ou fora de um prédio, conectado a um ser vivo, no mar, num campo de batalha, *etc.*.
A variação do contexto de funcionamento tem grande impacto no tipo de configuração de *hardware* e *software* do nó em questão pelo que deve ser assegurado a adequação do seu funcionamento às condições do ambiente alvo [11].

Topologia

As falhas recorrentes nos nós de sensores coloca um desafio importante à gestão de topologia nas redes de sensores. A instalação de um grande número de sensores implica que a densidade dos nós tenha um papel importante na gestão da topologia da rede.
Existem três fases que requerem a gestão e alteração da topologia da rede, a fase de pré instalação e instalação, a fase de pós instalação e a fase de reinstalação ou instalação de novos nós [11].

Na fase de **pré-instalação e instalação** os sensores podem ser colocados em locais pré-determinados ou simplesmente instalados nos locais onde são colocados aleatoriamente. Esta fase tem de ter em conta quatro pontos essenciais, optimização dos custos de instalação, criação de uma configuração ao nível de *hardware* e *software* que não necessite de uma pré-organização, maximizar a flexibilidade no arranjo da disposição física dos nós e promover a auto-organização e tolerância a falhas.

A fase de **pós-instalação** ocorre após a instalação dos nós no terreno. Nesta fase a topologia da rede pode variar por vários motivos, desde questões relaccionadas com a mobilidade, ruído do sinal, energia disponível, detalhes de funcionamento, *etc.*. Uma vez que os motivos que podem causar a falha de um nó da rede são muito variados, a probabilidade de acontecer é alta, assim, é expectável que seja necessário o re-arranjo da topologia da rede durante o funcionamento da mesma.

Finalmente, a fase de **reinstalação ou instalação de novos nós**, que ocorre sempre que um nó tem de ser substituído, reparado ou existe necessidade de instalar novos nós para recolha de informação sensorial. Estas alterações à rede implicam uma gestão da topológica da rede que, automaticamente, recupere o nó substituído ou inclua no seu encaminhamento o novo nó instalado.

Restrições de *Hardware*

Um nó de redes de sensores é composto tipicamente por quatro componentes básicos, uma unidade de sensor, uma unidade de processamento, uma unidade *transceiver* e uma unidade energética.

A unidade de sensor, é o equipamento físico que efectivamente transforma a informação referente ao fenómeno observado em sinais digitais para posterior processamento. A unidade de processamento gere os procedimentos que implicam a cooperação entre nós e verifica que o nó em questão efectua as tarefas que lhe foram atribuídas programaticamente. A unidade *transceiver* é a unidade que conecta o nó aos outros nós da rede. Por fim, a unidade de energia, a unidade que deve ser geralmente mais vigiada, pois suporta o funcionamento do nó em termos energéticos. A gestão desta unidade tem impacto directo na duração do funcionamento do equipamento. Para que um nó possa ter uma longevidade de bateria aceitável deve respeitar cinco pressupostos, baixo consumo de energia, deve operar em densidades volumétricas elevadas, deve ter um custo baixo e ser facilmente dispensável, ser autónomo e operar sem necessidade de intervenção humana e, finalmente, ser capaz de adaptar o seu funcionamento ao seu ambiente [11].

Meio de Transmissão

Os nós de comunicação de uma rede de sensores estão muitas vezes interligados pelo meio sem fio. No entanto, o tipo de ligação sem fio utilizado vai depender grandemente da aplicação da rede de sensores. Se o objectivo for a implementação de uma rede de sensores que possa abranger uma zona relativamente pequena, como sensores para monitorizar as condições de um campo relvado, podem ser utilizadas tecnologias como o *Bluetooth* ou o 802.15.4, por outro lado, se o fenómeno implicar uma área de observação maior, então o ideal é utilizar tecnologias que permitam um maior alcance como o WiMAX [11].
Embora o meio de transmissão seja uma componente fulcral, é também um dos factores que pesa bastante nos custos de produção devido à unidade *transceiver* cujo custo varia significativamente com a tecnologia usada [11].

Consumo Energético

Um nó sem fio da rede de sensores, é geralmente equipado com uma fonte de energia limitada dado às suas reduzidas dimensões. A gestão do consumo energético é uma questão que merece especial abordagem uma vez que a instalação dos nós em locais que nem sempre são de fácil acesso pode condicionar o seu funcionamento se os recursos não forem devidamente geridos dado que a substituição da bateria pode não ser possível. Por estes motivos, o período de "vida"de um nó de sensor está intrinsecamente ligado à capacidade da sua bateria.
O gestão do consumo energético é directamente influenciado por três tipos de tarefas que um nó geralmente executa, a monitorização do fenómeno, a comunicação e o processamento de dados [11].
A **monitorização do fenómeno** está relaccionada com a unidade de sensor. Esta unidade tem de ter em conta o tipo de fenómeno que se encontra a observar. Uma observação menos frequente implica uma utilização menos intensiva da bateria. Existem tipos de fenómenos que podem ser categorizados como mais dinâmicos, apresentando por isso uma necessidade de observação mais frequente (e.g. aceleração, luminosidade, *etc.*), enquanto que outros tipos de fenómenos podem requerer uma observação menos frequente (e.g. temperatura, humidade, *etc.*).
A **comunicação**, é a tarefa que tipicamente consome mais recursos energéticos uma vez que necessita de receber e enviar transmissões de dados com uma frequência elevada para manter o seu estado de operação actualizado.

O **processamento de dados**, por comparação com a tarefa de comunicação, apresenta um consumo energético significativamente inferior. O custo energético necessário para transmitir 1KB a 100m é aproximadamente o mesmo necessário para executar três milhões de instruções num processador MIPS que execute 100 milhões de instruções por segundo [11]. Perante esta informação, um bom processamento de dados, seleccionando os dados relevantes para transmissão, é bastante importante para a gestão de energia uma vez que evita a transmissão de dados irrelevantes. Por exemplo, se um sensor de luminosidade for afectado pela sombra temporária de um indivíduo que se encontre a passar pelo local, na caracterização do ambiente geral não faz sentido que essa súbita diminuição no valor de luminosidade seja tido em conta, pelo que, através de processamento de dados local, este dado possa ser descartado.

2.3.6 SunSpots

Na construção da rede de sensores incluída na prova de conceito da dissertação foram utilizados nós de rede sem fio SunSpots (ver Anexo B). Estes equipamentos foram escolhidos pela sua versatilidade e concordância com as premissas inerentes a um bom design de redes de sensores.
Estes dispositivos apresentam uma capacidade energética aceitável possibilitando um tempo de funcionamento considerável (ver B.2.3) e permitem uma fácil configuração através da *framework* que os acompanha. Utilizam a norma IEEE 802.15.4 que permite comunicações de curta distância e, uma vez que são compostos por sensores de ambiente, não se revela a necessidade de um maior alcance. Apresentam uma fácil instalação dadas as suas dimensões reduzidas e o hardware com que são equipados de origem é satisfatoriamente capaz.

2.4 Gestão de contexto

Os sistemas conscientes do contexto que os envolve dependem grandemente dos utilizadores e recursos que utilizam. A gestão de contexto tem como objectivo a optimização da ligação utilizando a rede para adaptar serviços e aplicações aos recursos e necessidades.

A gestão de contexto é tão bem sucedida quanto melhor forem executadas as três características fundamentais que a compõe, recolha de dados completa do ambiente, a correlação desses dados, e disponibilização da informação obtida [5].
A **recolha de contexto** é o mecanismo pelo qual a informação dos vários sensores é obtida pelo sistema de gestão de contexto.
A **correlação de dados** é o mecanismo que fornece ao sistema de gestão de contexto a camada de inteligência essencial para poderem ser feitas asserções reais sobre o ambiente que envolve a rede e é conseguida através do cruzamento entre a informação recebida de vários elementos.
A **distribuição de informação** é conseguida através de mecanismos que fazem chegar os dados recolhidos pela plataforma de gestão de contexto aos vários utilizadores.

2.4.1 Contexto

Embora as informações, tanto do utilizador como das aplicações sejam abundantes na rede, a interacção entre estes é estéril e não beneficia quer a utilização quer o objecto utilizado. Contexto pode ser considerada qualquer informação que permita caracterizar um evento ou

uma entidade. Uma entidade pode ser uma pessoa, um lugar ou objecto considerado relevante para a interacção entre o utilizador e a aplicação. O alvo da caracterização de contexto é promover a interacção utilizador-dispositivo a um nível simbiótico. O dispositivo interpreta a informação disponível sobre os gostos e preferências do utilizador providenciando-lhe os serviços que calcula serem os que melhor lhe aprazem. Por sua vez, o utilizador obtém, do dispositivo, informação relativa ao ambiente que o rodeia com o menor esforço possível, tendo apenas que especificar as suas preferências e, ao mesmo tempo que navega, consulta e utiliza serviços pode ser traçado um padrão que permita a extrapolação de um perfil.
O perfil contextual criado por um dispositivo vai influenciar a forma e o conteúdo da informação que passa a receber [14].

Categorização de contexto

A categorização do contexto permite o desenvolvimento de aplicações que possam seleccionar a informação de uma forma estruturada. A aplicação baseia-se nas questões "quem?", "onde?", "quando?"e "o quê?"sobre a entidade em foco para caracterizar um evento ou um pedido num determinado contexto [14].

Existem alguns tipos de contexto cuja relevância é superior e são considerados contexto primário na categorização de um ambiente, a localização, a identidade, a actividade e o tempo. Estes tipos de contexto não só respondem às quatro questões colocadas anteriormente mas também permitem, através do seu correlacionamento inferir sobre outros aspectos relativos à entidade utilizadora. A informação de contexto obtida através do correlaccionamento de informação de contexto primário são considerados contexto secundário. [14]

Divisão de contexto

Existem algumas propostas para a divisão de contexto em subtemas como, contexto de computação, contexto do utilizador, contexto físico [15] e contexto temporal [16].
O **contexto de computação** diz respeito à conectividade com a rede, aos custos associados, à largura de banda e aos recursos registados na rede (e.g. impressoras, *displays*, textitetc).
O **contexto do utilizador** refere-se ao perfil do utilizador, localização, entidades próximas e situação de redes sociais actual.
O **contexto físico** está relaccionado com as condições físicas do meio ambiente, tal como luz, temperatura, ruído, etc.
O **contexto temporal** categoriza a informação consoante a altura do dia, semana, mês e estação do ano.

Esta subdivisão permite caracterizar as actividades de uma entidade pesando vários factores e condições.

2.4.2 Integração de Contexto

A integração de contexto com a computação visa a automatização dos serviços prestados ao utilizador servindo as suas necessidades, de forma transparente, através de adaptação e reacção ao ambiente físico e computacional. [17]

A integração do contexto pode ser feita de duas formas, activamente e passivamente [16]. **Activamente**, através de aplicações que adaptam automaticamente o seu comportamento ao contexto que descobrem na rede. **Passivamente**, através de aplicações que guardam informação de contexto actual para uma posterior consulta.

2.4.3 Processamento Inteligente

Mesmo após a disponibilização da informação através as plataformas de contexto, existem alguns problemas quanto às tarefas que uma aplicação pode executar aquando do processamento da informação de contexto. Schilit define o processamento de contexto através da categorização de acções, selecção por proximidade, reconfiguração automática, comandos e informação contextuais e acções activadas por triggers [15].
A **selecção por proximidade** representa o recurso a uma tecnica onde os objectos localizados na vizinhança são colocados em evidência pela aplicação. A **reconfiguração automática** é um processo através do qual se gerem os componentes da aplicação e se alteram as ligações devido a alterações de contexto. Os **comandos e informação contextuais** são formas de produzir resultados diferentes por um mesmo processo. Os resultados/informação produzida variam consoante o contexto em que se encontram. As **acções activadas por triggers** são comparações simples entre valores pre-determinados e valores recebidos a cada momento, retirados do contexto. A utilização desta definição permite a adaptação das aplicações.

Em ultima análise, a gestão de contexto, permite reunir informação de várias origens (e.g. sensores, equipamentos móveis, utilização da rede, *etc.*), e com estes dados construir uma camada de inteligência interligando informação que permita inferir algumas características sobre os utilizadores e o meio. Após disponibilização da informação recolhida, os utilizadores podem aceder-lhe por meio de aplicações independentes ou através de aplicações mais complexas embutidas em mecanismos que utilizem o contexto para efectuar decisões. [14]

2.5 IEEE Standard 802.21 MIH

A norma IEEE 802.21 *Media Independent Handover* surge no panorama do IEEE como forma de optimizar o processo de *handover* entre redes heterogéneas IEEE 802 e facilitar o mesmo entre redes IEEE 802 e redes celulares através de mecanismos independentes de acesso ao meio.

O objectivo desta norma é proporcionar uma melhoria na experiência aos utilizadores de dispositivos móveis possibilitando um *handover* transparente entre redes, independentemente da forma de acesso ao meio (sem fio ou por cabo), onde outrora não existia. A abstracção criada por este protocolo é essencial para uma imersão contínua do utilizador nas suas tarefas, não o importunando com questões de ligação uma vez que esta norma facilita a gestão da mesma [1].

O *handover* é optimizado com base em duas fontes, a informação recolhida da rede e alguma inteligência ao nível da camada de ligação providenciada pela norma em si, que é, à posteriori, enviada para as camadas superiores, onde é processada e pode gerar uma decisão de *handover* optimizada.

Para utilizadores móveis, um *handover* pode ocorrer quando as condições da ligação se alteram devido à movimentação do utilizador ou às características da rede, tornando outra rede mais atractiva ou contextualmente preferível.

Todos os aspectos já referidos relaccionam-se directa ou indirectamente com a optimização da continuidade de serviços, característica que deve ser preservada o mais possível durante um *handover*. Imagine-se o seguinte cenário, um utilizador está a fazer uma chamada, independentemente do meio e forma, e a rede à qual está ligado deixa de suportar a sua ligação. Existindo, em *overlap*, outra rede que providencie o mesmo serviço, o ideal é que o dispositivo móvel efectue o *handover* da forma mais transparente possível para o utilizador e a interrupção na conversação seja minimizada [1].

A troca de informação é efectuada recorrendo à cooperação entre os nós móveis da rede e a própria infraestrutura da rede. Esta cooperação é garantida recorrendo a dois pressupostos. Os nós móveis asseguram uma posição vantajosa abrangendo o maior número possível de redes disponíveis e a infraestrutura da rede está equipada para guardar informação global (e.g. listas de células vizinhas, posicionamento dos nós móveis, estado e disponibilidade das camadas superiores suportadas). Todas as decisões podem ser tomadas bi-lateralmente e a comunicação da informação recolhida pelo nó móvel à rede e vice-versa é essencial. É ainda expectável, que ambas as partes possuam componentes multi-modais, ou seja, possam suportar múltiplos tipos de *standards* rádio e simultaneamente suportem conexões em duas ou mais interfaces [1].

Tal como o nome *Media Independent Handover Services*, sugere, os elementos constituintes da infraestrutura de uma rede podem ser do mais diverso e heterogéneo possível (e.g. IEEE 802.15, 802.11, 802.16, 3GPP e 3GPP2) uma vez, e desde que, a cobertura seja feita em *overlap*, caso contrário a continuidade da ligação deixa de ser assegurada. O processo de *handover* pode ser iniciado por eventos, com informação relativa à camada de ligação, que são despoletados através de triggers e temporizadores. De entre várias configurações suportadas, em cenários onde, por exemplo, exista uma pré-configuração de um limiar para a potência de sinal mínima recebida, sempre que esse limiar for ultrapassado é reportado o evento respectivo, permitindo à rede iniciar um *handover* para uma célula que comporte os requerimentos mínimos do nó móvel em questão. Igualmente, podem ser configurados temporizadores para que a informação desejada seja transmitida periodicamente ou mesmo serem efectuados pedidos instantâneos, do tipo pergunta-resposta para actualizar o estado dos elementos constituintes. A informação reportada pode conter vários tipos de conteúdo, desde qualidade de sinal, taxas de transmissão de erro, informação da interface,*etc.* [1].

Estrutura geral

Funcionalmente, este protocolo pode ser considerado uma estrutura tri-partida. Definem-se os três elementos principais como sendo modelos de referência, MIH SAP, MIHF e MIH User [1].
Conjuntamente com estes elementos a norma especifica ainda a interacção entre os mesmos e baseia-se nos seguintes pressupostos:

- Existência de uma *framework* que garanta a continuidade de serviço de um nó móvel aquando de uma transição entre tecnologias heterogéneas ao nível da camada de ligação.

Para este efeito a *framework* baseia-se na presença de uma *stack protocolar* de gestão de mobilidade situada nos elementos da rede que suportam o processo de *handover*.

- Um conjunto de funções que suportam e permitam o *handover* internamente com as *stacks protocolares* de cada elemento da rede juntamente com a respectiva MIHF.

- Utilização de um MIH SAP (media *handover* service access point) que providencia aos MIH Users uma interface de acesso aos serviços existentes na MIHF.

- Cada MIHF dispõe de SAPs de ligação que em conjunto com as primitivas de cada tecnologia permitem ao MIHF reunir informação e controlar o comportamento da ligação durante o *handover* denominadas LINK SAPs.

- A MIHF define três tipos de serviços distintos, o serviço de comandos (MICS), de eventos (MIES) e de informação (MIIS). A existência destes três serviços é a base para um processo de *handover* o mais transparente e eficiente possível.

Para que as entidades funcionais desempenhem o seu papel é essencial que exista a comunicação apropriada entre os mesmos. Esta é garantida pelo protocolo MIH que define o formato das mensagens a serem trocadas entre os vários mecanismos independentes do meio presentes na rede e as entidades MIHF. O protocolo MIH define exaustivamente, dentro do formato das mensagens, a sua forma de codificação, estrutura e regras de implementação por forma a manter coerência na comunicação.

A figura 2.2 demonstra um exemplo da interacção dos serviços com as diversas entidades do protocolo. Demonstra ainda os mecanismos de comunicação definidos pelo IEEE 802.21 onde a MIH SAP serve de interface entre a MIHF e os MIH Users. Para as camadas mais baixas da *stack protocolar* a MIHF comunica através de MIH SAPs específicos que dependem do meio de comunicação, representados na figura por MIH LINK SAP.

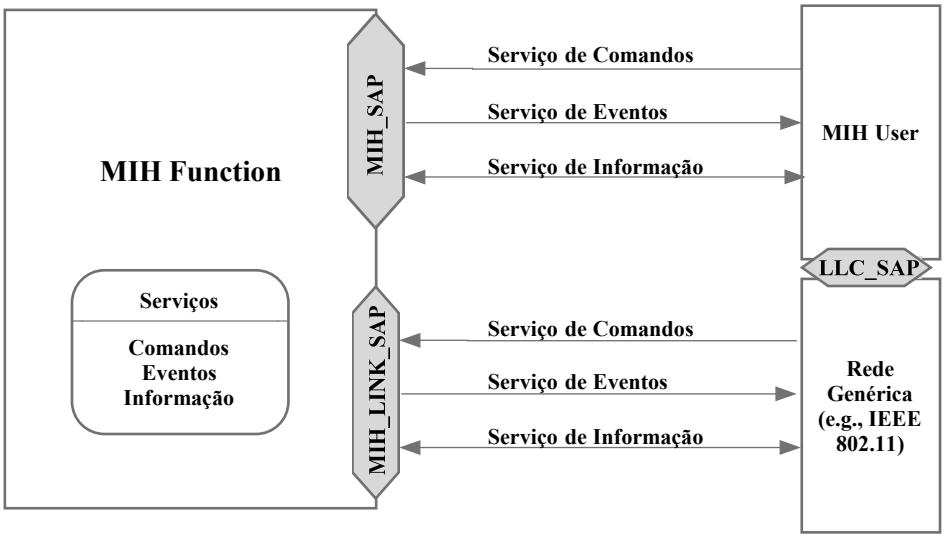


Figura 2.2: Interacção de Serviços MIH

2.5.1 MIHF - Media Independent Handover Function

A MIHF é uma entidade lógica com a função de facilitar o processo de *handover* bem como todas as operações associadas. A decisão de iniciar o processo de *handover* é da responsabilidade do MIH User que se baseia em informação recolhida através da MIHF.
Actuando como intermediária entre SAPs específicos e MIH User, a MIHF gere toda a comunicação e operação subjacente, criando uma abstracção dos serviços existentes para as camadas superiores [1].

Princípios gerais de funcionamento da MIHF

- Implementa e disponibiliza meios para auxiliar os MIH Users a manter a continuidade de serviço, seja, fornecendo formas inter-tecnológicas de simplificação de adaptação dos serviços à qualidade de ligação, gerindo o ciclo de vida de baterias, descoberta de redes ou escolha de ligações.
- Define serviços síncronos e assíncronos através de SAPs para os MIH Users e para a camada de ligação. Em situações em que existam múltiplas interfaces de rede os MIH Users podem controlar o estado das mesmas pelos serviços de eventos, comandos e informação de forma tecnologicamente independente.
- Providencia, suporte remoto para eventos, comandos e informação do protocolo MIH, gerados em outros nós da rede mediante prévio registo/subscrição.
- Em cenários onde existam interfaces de redes heterogéneas IEEE 802 e redes celulares, a MIHF assiste o MIH User na implementação de procedimentos que permitam interligar os serviços. Os MIH Users utilizam também a MIHF, remota ou local, para requisitar informação sobre recursos de redes.
- Os serviços MIH em nós móveis facilitam os procedimentos de *handover* mascarando a complexidade e a mudança de ligação.

Serviços MIH implementados pela MIHF

Os serviços MIH permitem que os processos de *handover* decorram da forma mais transparente possível entre redes heterogéneas uma vez que definem uma gama de operações e mensagens bastante completos que facilitam a difusão de informação e controlo em múltiplos cenários. Os três tipos de serviços já referidos, além de facilmente extensíveis, não são exclusivos, querendo com isto dizer, que podem ser acedidos por vários tipos de MIH User e não apenas por protocolos de gestão de mobilidade (e.g. Mobile IP).

MIES - Media Independent Event Service

Este serviço detecta alterações nas condições da ligação e despoleta os eventos apropriados. Este tipo de eventos são baseados em limiares de transpassamento configurados com um valor e uma direcção, cada vez que o valor obtido atravessar o valor e direcção configurados é gerado um evento para este efeito. Cada evento pode ter um contexto local ou remoto e apenas existe no sentido MIH SAP para MIH User. Providencia também a classificação e filtragem de eventos assim como o despoletar dos mesmos quando existem alterações dinâmicas nas características, estado ou qualidade da ligação.

Os eventos podem ter várias origens, pelo que podem ser referenciados como locais ou remotos. Este serviço permite a existência de várias entidades interessadas num evento ao mesmo tempo. Para esse propósito, um evento pode ter múltiplos destinos além de que entidades de camadas superiores podem subscrever um determinado evento, de origem específica, para receberem notificações do mesmo.

O IEEE 802.21 classifica os eventos como tendo uma natureza de "advertência"e não "mandatória"uma vez que o destinatário não é obrigado a actuar sobre cada mensagem que recebe. A fiabilidade dos eventos recebidos e a robustez dos mesmos, é encargo das entidades pertencentes à camada três (*network layer*) e acima, pelo que é especificado ainda no mesmo *standard* que essas entidades deverão tomar uma posição mais apreensiva e cautelosa a eventos remotos em detrimento dos eventos gerados localmente.

Existem dois tipos de categorias no serviço de eventos, eventos de ligação (Link Events) e eventos MIH (MIH Events). Ambos atravessam as camadas protocolares forçosamente no sentido da camada mais baixa para a mais alta (ver figuras 2.3 e 2.4). Os **Link Events** definem-se como sendo eventos originados por entidades abaixo da MIHF. As entidades que geram estes eventos podem ser de variadas interface (e.g. IEEE 802, 3GPP, 3GPP2, *etc.*). Os eventos são enviados para a MIHF que, internamente, com ou sem processamento, os propagará para MIH Users que subscreveram o evento em causa. Tipicamente todos os eventos de ligação são locais.
Os **MIH Events** são eventos originados pela MIHF ou apenas Link Events que são propagados pela MIHF para os MIH Users. Este tipo de eventos podem ser locais ou remotos.

Fluxo do Serviço de Eventos

Como previamente apresentado, um evento pode ser local ou remoto. Um evento local é um evento que se propaga por várias camadas dentro de uma *stack* protocolar local de uma entidade MIH, encontrando-se esta relação representada pela figura 2.3.

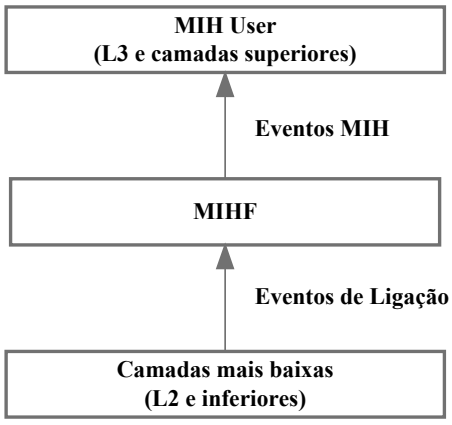


Figura 2.3: Eventos locais

Eventos remotos são eventos que atravessam o meio da rede entre uma MIHF remota e uma MIHF local. Esta relação encontra-se demonstrada pelo exemplo da figura 2.4 onde se

pode observar a existência de um evento de ligação com origem nas camadas inferiores e é encaminhado para a MIHF local. Após processamento interno, é propagado um evento MIH para a MIHF remota que propaga o mesmo para o MIH User.

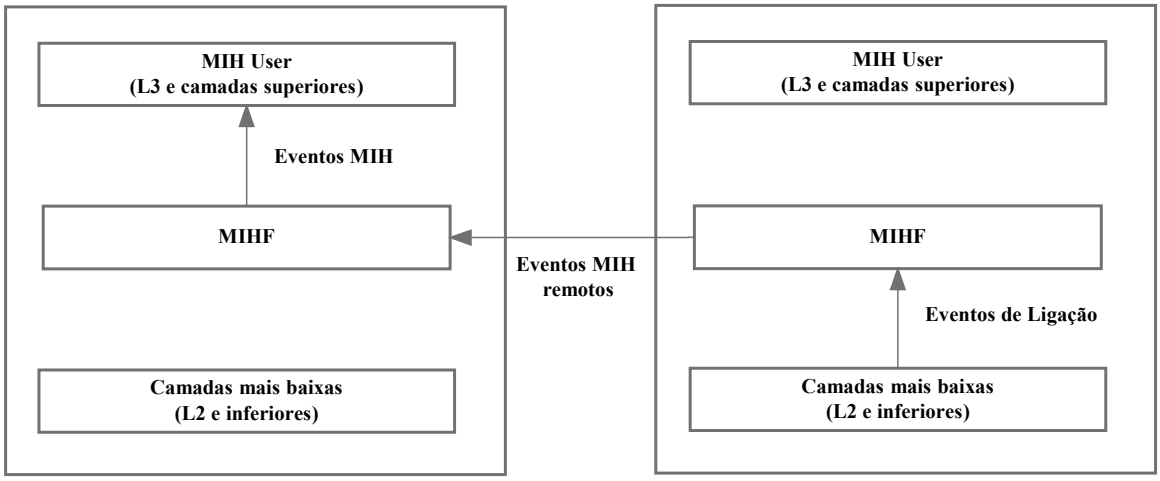


Figura 2.4: Eventos remotos

MICS - Media Independent Command Service

O serviço de comandos, especifica uma colecção de comandos para que os MIH Users possam controlar e gerir as propriedades da ligação. Este serviço permite que os MIH Users enviem comandos para as camadas mais baixas. Pode iniciar e controlar procedimentos de *handover* para controlar o balanceamento da carga da rede.
O estado e qualidade da ligação variam ao longo do tempo e consoante a movimentação do nó movel (MN), impondo que a informação fornecida pelo serviço de comandos tenha uma natureza maioritariamente dinâmica. Alguns parâmetros que compõe essa informação são altamente relativos ao contexto de mobilidade e às condições do ambiente, como a força de sinal e velocidade da ligação, entre outros. Todos os comandos são mandatórios por natureza, pelo que quando a MIHF recebe um comando espera-se que o execute. Alguns comandos MIH podem despoletar de eventos que servem para notificar os MIH Users de que algo se alterou ou está prestes a alterar.

O serviço de comandos divide-se em duas categorias, comandos MIH e comandos de ligação, que se definem segundo a interacção com a MIHF e as camadas envolventes, os Link Commands e os MIH Commands.
Os **Link Commands** são comandos originados na MIHF e enviados para as camadas mais baixas. Estes comandos são, por norma, utilizados para controlar o comportamento das entidades das camadas mais baixas. Embora estes comandos sejam originados na MIHF e apenas existam no contexto local, são os MIH Users que ordenam a sua execução.
Os **MIH Commands** são comandos gerados por MIH Users e enviados para a MIHF, podendo existir num contexto local ou remoto. Os comandos MIH locais são enviados pelo MIH User para a MIHF da *stack* protocolar local.

Fluxo do Serviço de Comandos

À semelhança do serviço de eventos, o serviço de comandos pode ter uma natureza local ou remota. Um comando local propaga-se desde os MIH Users para a MIHF e é depois direccionado para as camadas mais baixas, tal como retratado na figura 2.5.

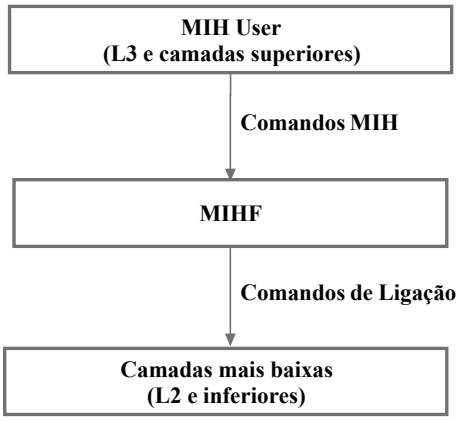


Figura 2.5: Comandos locais

Com os comandos remotos, as mensagens propagam-se desde o MIH User para o MIHF na mesma *stack* protocolar e são depois enviadas para o MIHF de uma *stack* protocolar remota através do protocolo MIH, seguindo o esquema da Figura 2.6.

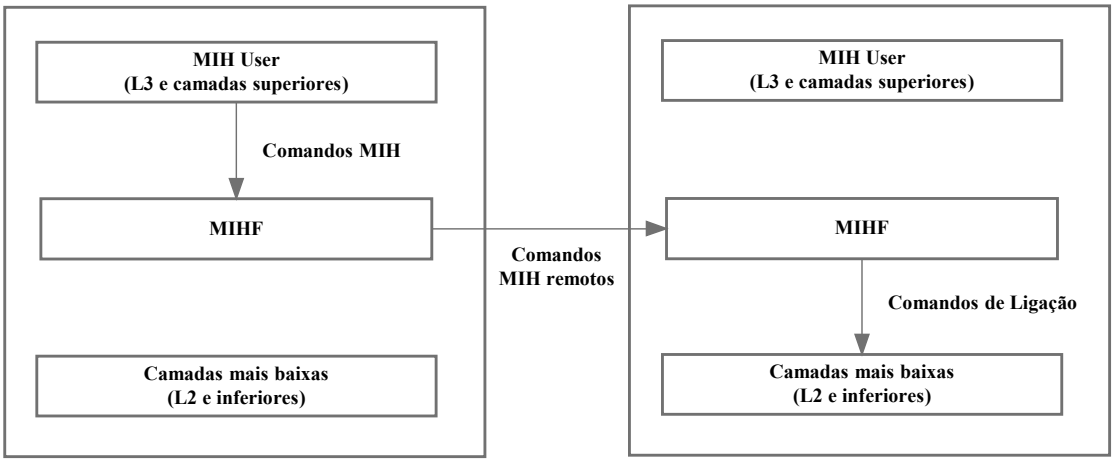


Figura 2.6: Comandos Remotos

MIIS - Media Independent Information Service

O serviço de informação, disponibiliza mecanismos que permitem obter e descobrir informação sobre diferentes redes e os respectivos serviços. A informação reunida sobre redes vizinhas e os mecanismos implementados por este serviço, em conjunção com o utilizador e os parâmetros do operador de rede, permitem uma melhor escolha na selecção de redes conseguindo melhorar a performance do processo de *handover*.

O serviço de informação disponibiliza ainda um conjunto de elementos de informação (*Information Elements*), a estrutura e representação da informação e um mecanismo de pergunta/resposta para a transferência de informação. Existem dois tipos de acesso/recolha de informação, *pull* e *push*. *Pull* serve para obter a informação do servidor MIIS e *push* para colocar informação no servidor MIIS, geralmente utilizado pelo operador da rede.
A informação pode existir num servidor de informação onde o MIHF e o MN podem aceder, ou pode só existir localmente no MN.

O acesso à informação está disponível tanto pelas camadas mais baixas como mais altas. Em certos cenários, a informação disponível na L2 não é suficiente para uma tomada inteligente de decisão quanto ao processo de *handover*. Nestas situações a informação pode ser acedida através de camadas superiores. Por estes motivos, o protocolo MIH 802.21 permite o acesso a informação via L2 e L3 [1].

Tipicamente, a informação providenciada por este serviço tem um teor bastante estático uma vez que é composta por informação relativa a parâmetros como operadores de redes ou informação relativa a serviços de camadas superiores. O MIIS especifica a forma de representação da informação através das várias tecnologias, usando formatos normalizados como o XML ou codificação binária. A estruturação da informação nos formatos referidos define-se por *schema*.

Algumas redes, como as redes celulares, já possuem meios para detectar uma lista de redes na vizinhança via controlo de canais *broadcast*. Outras normas IEEE definem ainda meios similares de detecção tanto por *beaconing* como por *broadcast* de mensagens de gestão MAC, *etc.*.
O MIIS define um mecanismo unificado para as entidades de camadas superiores providenciando informação relevante para o processo de *handover* numa rede heterogénea dependendo da sua localização em relação à rede. Em última análise, o sistema de informação tem como objectivo auxiliar os protocolos de mobilidade de camadas superiores a adquirir uma vista global das redes heterogéneas permitindo ao processo de *handover* tornar-se o mais transparente e com menor impacto possível ao longo das redes [1].

Fluxo do Serviço de Informação

O fluxo do sistema de informação não possui mensagens que tenham necessariamente uma natureza de ligação. As mensagens do sistema informação mantêm-se iguais seja qual for o contexto, local ou remoto. Isto significa que, uma mensagem que chegue à MIHF vinda do MIH User não sofre alterações na sua estrutura. A mensagem é apenas redireccionada para o seu destinatário.
Em situações onde a mensagem apenas existe entre o MIH User e a sua MIHF local, a mensagem não transita para fora da *stack* protocolar, podendo dizer-se que esta mensagem tem um carácter local. Existe também a possibilidade da mensagem ser enviada de um MIH User para outro MIH User remoto, nesta situação as mensagens são enviadas para as MIHFs locais a cada MIH User que se encarregam de as redireccionar remotamente. Por comparação, podemos inferir que ao contrário dos sistemas de comandos e eventos, a natureza da ligação é transparente às mensagens do sistema de informação [1].

A figura 2.7 representa um possível modelo de fluxo de comunicação para uma situação em que as comunicações sejam meramente locais, ou seja, as mensagens apenas se propagam entre o MIH User e a MIHF local.

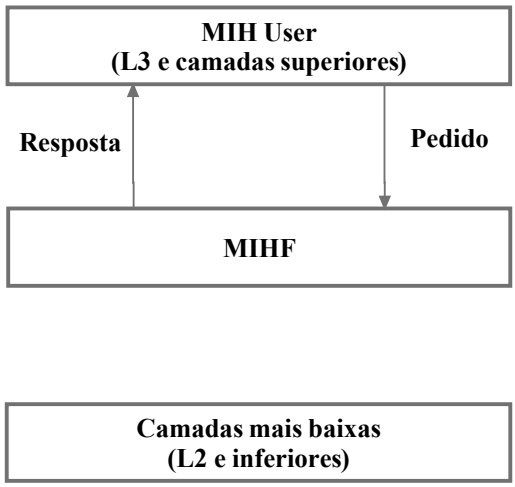


Figura 2.7: Fluxo de Sistema de Informação local

A figura 2.8 demonstra um modelo de fluxo de comunicação onde as comunicações são efectuadas remotamente. As mensagens atravessam entre a rede, de um MIH User para outro MIH User sendo redireccionadas pelas MIHF.

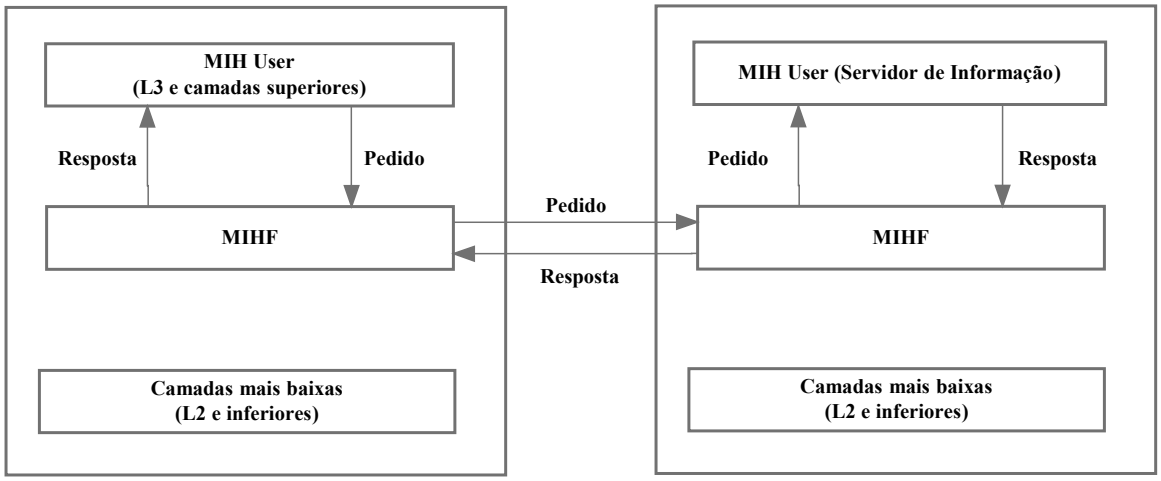


Figura 2.8: Fluxo de Sistema de Informação remoto

2.5.2 Modelo de Comunicação

O modelo de comunicação descreve os elementos de comunicação relativamente aos pontos chave existentes nas entidades MIHF, MN e da própria rede. A relação entre os vários elementos referidos pode ser representado pela figura 2.9. Demonstrando como um exemplo onde um MN comunica com uma rede que suporta MIH 802.21.

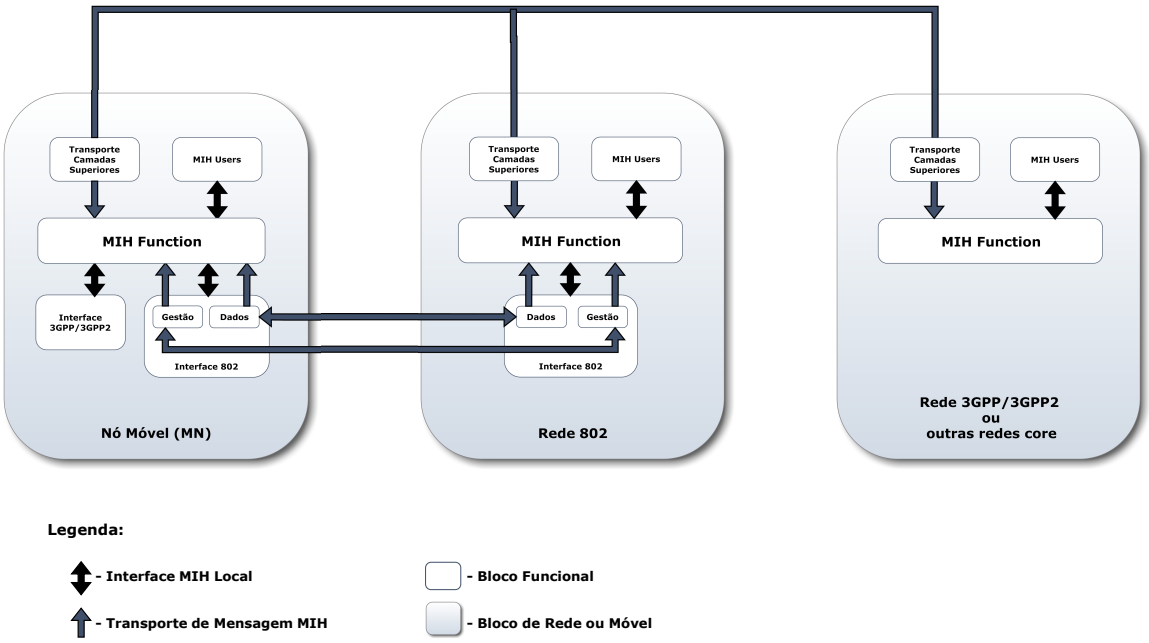


Figura 2.9: Modelo conceptual de relações

2.5.3 Pontos de Comunicação

Existem duas notações que caracterizam as entidades do modelo de comunicação e a sua relação, *point of service* (PoS) e *point of attachment* (PoA).

Point of Service - PoS

O MN troca informação directamente com o seu MIH PoS. A MIHF em qualquer entidade da rede torna-se um PoS quando comunica directamente com uma MIHF de um MN. Quando uma MIHF de uma entidade de rede não tem ligação directa com o MN, mesmo que comunique por alguma forma com este, não se intitula o seu PoS. Uma entidade de rede pode ter várias ligações, pelo que para uns elementos pode ser PoS mas para outros pode já não reunir características para o ser.

Point of Attachment - PoA

Um MN pode ter múltiplas interfaces L2, no entanto, a comunicação com entidades MIHF não necessita de ocorrer em todas estas interfaces. Sendo que, se um MN possuir duas

interfaces, uma pode ser utilizada para o uso de serviços da MIHF e a outra para administração de sistema ou outro tipo de operações. Um MN pode usar transporte via L2 para trocar informação com um PoS que resida na mesma entidade de rede que o seu PoA. Pode também usar transporte via L3 para trocar informação com um PoS que não resida na mesma entidade de rede que o seu PoA. A MIHF pode ter comportamentos distintos dependendo da sua posição na rede em relação às outras entidades:

- Assume papel de MIH PoS na entidade de rede que inclui o PoA de serviço para um determinado MN.
- Assume papel de MIH PoS na entidade de rede que não inclui o PoA de serviço para um determinado MN.
- Assume papel de MIH não PoS na entidade de rede que não inclui o PoA de serviço para um determinado MN

O modelo de comunicações define tipos de ligação diferentes dependendo do comportamento da MIHF:

Tipo de Ligação 1 - Procedimentos entre a MIHF do MN e o MIH PoS da entidade de rede que lhe serve como PoA. O conteúdo desta ligação pode pertencer aos vários serviços suportados, MICS, MIES e MIIS.

Tipo de Ligação 2 - Procedimentos entre a MIHF do MN e o MIH PoS da entidade de rede que é considerado candidato PoA. O conteúdo desta ligação pode pertencer aos vários serviços suportados, MICS, MIES e MIIS.

Tipo de Ligação 3 - Procedimentos entre a MIHF do MN e o MIH PoS de uma entidade de rede não PoA. Pode ser utilizado como ligação para protocolos de transporte de L2 (e.g. MPLS). O conteúdo desta ligação pode pertencer aos vários serviços suportados, MICS, MIES e MIIS.

Tipo de Ligação 4 - Procedimentos entre um MIH PoS de uma entidade de rede e um MIH não PoS de outra entidade de rede. O conteúdo desta ligação pode pertencer aos vários serviços suportados, MICS, MIES e MIIS.

Tipo de Ligação 5 - Procedimentos entre dois MIH PoS em entidades de rede diferentes. O conteúdo desta ligação pode pertencer aos vários serviços suportados, MICS, MIES e MIIS.

Os TPL1, TPL2 e TPL3 suportam comunicações de interfaces sobre L2, L3 e acima, enquanto que os TPL4 e TPL5 apenas suportam comunicações acima de L3.

O modelo de comunicações pode ser ilustrado através da figura 2.10. Pode observar-se que existem representados 5 tipos diferentes de interligação entre elementos MIH da rede, em congruência com os tipos de ligação existentes.

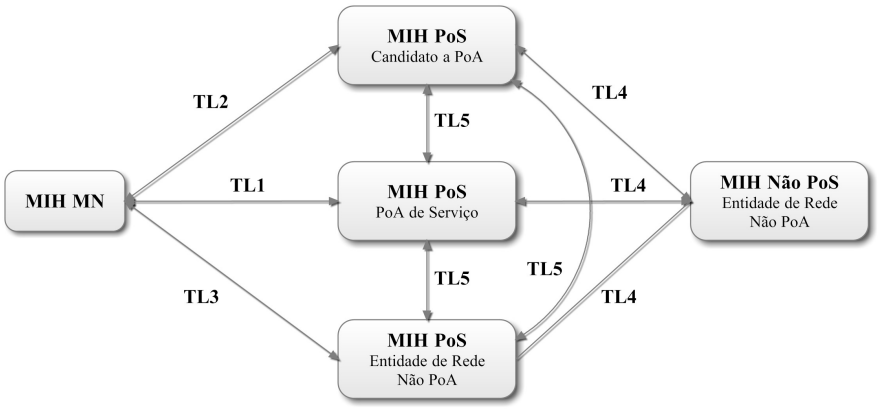


Figura 2.10: Modelo de Comunicação

Modelo de Comunicação Exemplificativo

A figura 2.11 representa um exemplo de modelo de comunicação com os vários tipos de ligação e diferentes entidades.

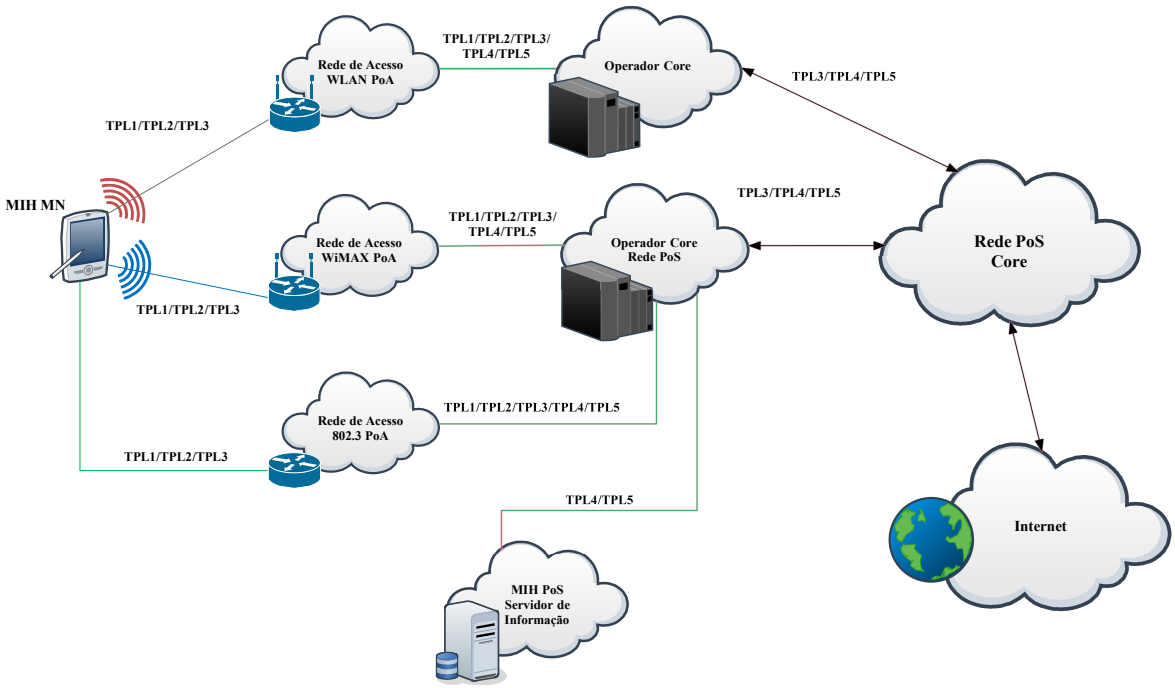


Figura 2.11: Modelo de Comunicação Exemplificativo

Verifica-se que o MN suporta várias interfaces ligadas a várias redes de acesso que se conectam a operadores de rede core. A ligação com a internet é feita por meio de uma rede core central que está interligada aos operadores de rede. Numa das redes existem um servidor de informação ilustrando o uso do MIIS. Todas as outras ligações representam ligações com suporte os vários serviços, MIES, MICS e MIIS. O MN utiliza interfaces e conexões inter-tecnologia criando redundância de ligação, garantindo efectivamente uma conectividade que suporte os seus requisitos.

2.5.4 SAP - Service Access Points

A interface entre a MIHF e os planos de comunicação é conseguida através de pontos de acesso a serviços (SAPs). A especificação da MIHF inclui a definição de SAPs, independentes do meio, advertindo para a necessidade e importância da definição de outros SAPs, dependentes do meio. Os SAPs independentes do meio permitem que a MIHF forneça serviços para as camadas superiores das camadas protocolares de gestão de mobilidade, gestão de rede e suporte de dados. Entidades de camadas superiores necessitam de se subscrever com a MIHF, como MIH Users, para que possam receber eventos gerados tanto pela MIHF como eventos relacionados com a ligação gerados nas camadas a baixo da MIHF. Os MIH Users enviam comandos directamente para a MIHF local usando as primitivas de serviço da MIH SAP. A comunicação entre duas MIHFs depende das mensagens de protocolo MIH [1]. Os SAP podem ser definidos por conjuntos de primitivas. Cada conjunto de primitivas define um serviço. As primitivas são compostas por uma tabela de parâmetros permitidos onde cada parâmetro é definido utilizando tipos de dados abstractos. Os tipos de dados abstractos definem o valor semântico de cada parâmetro. De um modo geral , a MIHF utiliza os SAP como forma de interface com outras entidades pelo que actuam como tradutores entre os meios de comunicação e as respectivas entidades. Os SAP podem ser categorizados e distinguidos pela sua dependência ao meio.

SAPs dependentes do meio

Os SAPs dependentes do meio permitem que a MIHF utilize serviços específicos pertencentes às camadas mais baixas da camada protocolar. Todos as entradas vindas das camadas mais baixas para a MIHF só são passíveis de atravessar para o seu destino porque existem SAPs específicos para cada meio utilizado (e.g. MAC SAP, PHY SAP, LLC SAP).
Cada tecnologia de ligação especifica o seu próprio SAP. O MIH LINK SAP mapeia cada SAP para a sua respectiva tecnologia de ligação.
O **MIH LINK SAP** implementa uma interface abstracta com dependência ao meio e é utilizada pela MIHF para comunicar com as camadas mais baixas da stack protocolar específica para cada meio.
O **MIH NET SAP** implementa uma interface com dependência ao meio e é utilizada pela MIHF para serviços de transporte sobre a camada de dados no nó local suportando a troca de informação e mensagens MIH com a MIHF remota.

SAPs independentes do meio

Definem uma interface independente do meio entre a MIHF e os MIH Users. Este elemento é essencial à definição e especificação da MIHF. O **MIH SAP** representa a interface entre a MIHF e os MIH Users e é independente do meio.

A figura 2.12 ilustra um exemplo da posição que os vários SAPs possuem em relação à MIHF e aos outros elementos da *stack*.

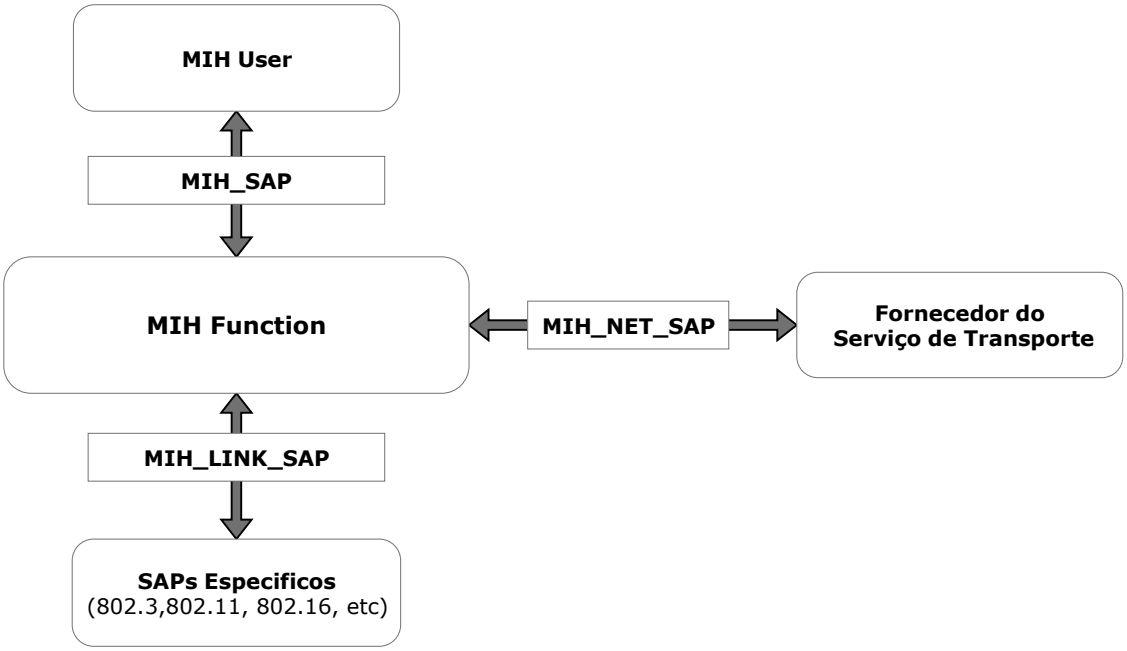


Figura 2.12: Relações entre SAPs e outros elementos da rede.

2.5.5 MIH Users - Utilizadores MIH

Os MIH Users são elementos pertencentes a entidades de rede que fazem uso da informação e são, em última análise, a razão de existir todos os mecanismos e outros elementos que fazem parte desta norma. São os utilizadores que originam os comandos e recebem as respostas aos mesmos, colocando em movimento todo o protocolo que lhe é inerente.

Em situações de *handover*, são os MIH Users que tratam de controlar o estado da ligação, gerindo, a todo o instante, por forma de comandos, eventos e mensagens do sistema de informação, se é necessário efectuar um *handover* ou se a ligação possui os requisitos necessários para se manter.

O MIH User acede a todo o tipo de informação que a MIHF lhe disponibiliza relativamente a outras entidades de rede. Por este motivo, pode ter vários usos para além de controlar todos os processos inerentes ao *handover* uma vez que ao concentrar informação de outros elementos da rede se gera automaticamente uma camada de inteligência que pode vir a servir outros propósitos.

2.5.6 Protocolo MIH

As MIHF pertencentes aos MN e às entidades de redes comunicam entre si trocando mensagens de protocolo MIH. O protocolo MIH define o formato das mensagens que são trocadas entre entidades MIHF remotas. As mensagens são baseadas em primitivas que fazem parte dos serviços MIH.

Transporte

O transporte de mensagens de protocolo MIH é feito através do plano de dados usando mecanismos de transporte adequados tanto na camada 2 como na camada 3. Na camada 3 o transporte é suportado usando TCP/UDP/SCTP por IP. Para a camada 2 o transporte é suportado marcando o valor Ethertype para esse efeito no protocolo MIH. O EtherType é uma forma de identificar todas as unidades de dados do protocolo MIH. O plano de dados está disponível para transporte apenas depois do MN se autenticar com a rede de acesso. Em casos como redes IEEE 802.11 ou IEEE 802.16 as mensagens de protocolo MIH podem ser trocadas antes da autenticação através do plano de gestão usando tramas de gestão MAC.

Formato da trama protocolar MIH

As mensagens MIH codificam os seus parâmetros em formato TLV (type, length, value). A figura 2.13 demonstra a representação da codificação de um parâmetro genérico. Cada parâmetro é composto por três componentes, Type que representa o tipo do parâmetro, pertencente a uma lista conhecida de valores onde a cada valor corresponde um parâmetro único, Length possui a informação do tamanho do parâmetro e Value que possui os dados relativos ao parâmetro.

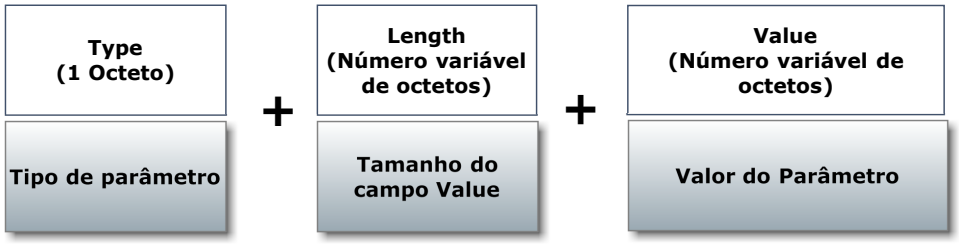


Figura 2.13: Codificação TLV.

Cada mensagem é composta por um cabeçalho (*header*) e o respectivo conteúdo (*payload*). O protocolo MIH define que cada *payload* seja constituído pelo identificador da MIHF fonte, pelo identificador da MIHF destino seguidos pelos parâmetros respectivos para cada tipo de mensagem, codificados no formato TLV. A figura 2.14 representa uma trama genérica de uma mensagem MIH.

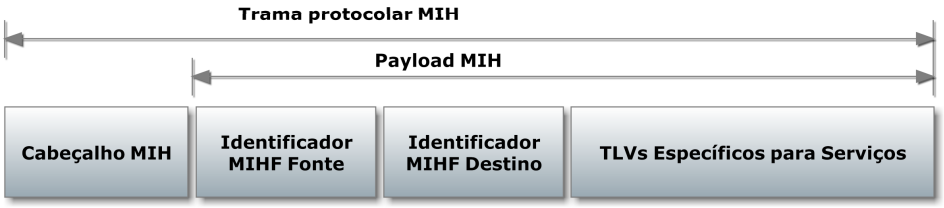


Figura 2.14: Trama Protocolar MIH.

O cabeçalho de cada mensagem MIH possui informação essencial para uma correcta transferência de dados e está presente em todas as tramas sendo utilizado para fazer o *parsing* da trama em si. A figura 2.15 ilustra a sua composição [1].

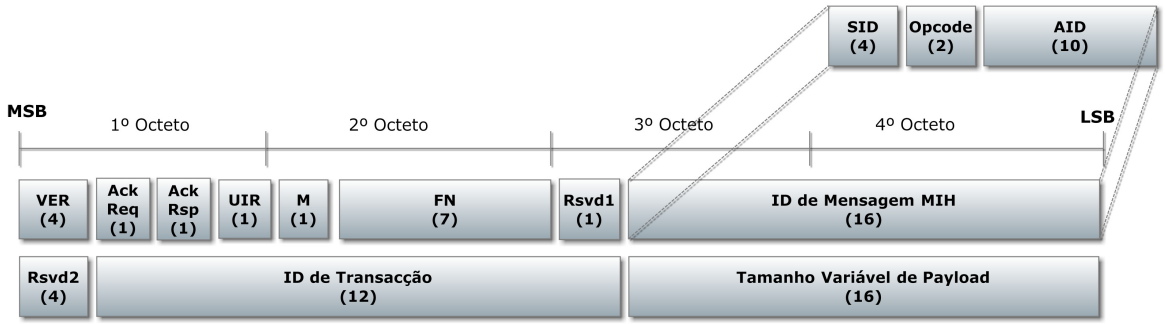


Figura 2.15: Cabeçalho da trama protocolar MIH

2.5.7 Serviços MIHF

Os serviços MIH (MICS, MIES, MIIS) que permitem e facilitam o *handover* entre redes heterogéneas são geridos e controlados através de primitivas de gestão.

Gestão de Serviços

Para que as entidades MIH possam providenciar os serviços MIH entre MIHFs distintas é necessário que exista uma configuração correcta. A gestão de serviços é executada através das seguintes funções:

- Descoberta de Capacidades MIH (MIH Capability Discover)
Procedimento utilizado por um MIH User para descobrir as capacidades de MIHF's locais ou remotas. Este procedimento pode ser efectuado via protocolo MIH ou por mecanismos específicos de cada meio (e.g. *beacon frames* de IEEE 802.11, mensagens de gestão IEEE 802.16, *etc.*).

- Registo MIH (MIH Resgister)
O Registo MIH é definido como um mecanismo para acesso a serviços MIHF específicos que necessitem de algum controlo sobre os utilizadores.

- Subscrição de Eventos MIH (MIH Event Subscription)
O mecanismo de subscrição de eventos possibilita ao MIH User subscrever um conjunto específico de eventos originados na MIHF local ou remota.

As entidades MIH só podem descobrir e conhecer as capacidades dos seus pares através de primitivas MIH Capability Discover. Após a execução destas primitivas, a entidade MIH descobre as capacidades inerentes a cada entidade MIH e assim pode decidir com qual se registar. A partir do momento em que se regista com uma determinada entidade MIH, subscreve os eventos que esta suporta por forma a receber as notificações que lhe aprouverem.

Comunicação por rede

Existem funções que permitem a comunicação entre entidades MIH por rede providenciando serviços de transporte através do plano de dados do nó local suportando a troca de informação MIH e mensagens entre MIHFs locais ou remotos. Para serviços de transporte por L2, a MIH NET SAP utiliza as primitivas especificadas pelo MIH LINK SAP. Em serviços de transporte por L3, as primitivas são especificadas pelo MIH NET SAP.

2.6 XMPP - Extensible Messaging and Presence Protocol

O XMPP é um protocolo de tecnologia aberta para comunicações de tempo real. Presentemente este protocolo é utilizado numa vasta gama de aplicações desde informação de presença, mensagens instantâneas, *chat multi-party*, chamadas de vídeo e voz, publicação de conteúdos, encaminhamento generalizado de dados XML, *etc.*.
Tipicamente o XMPP é utilizado para interacções do tipo pergunta-resposta. Sendo um protocolo baseado em XML as mensagens são construídas em conformidade com as regras que lhe são intrínsecas.
O IETF formalizou o XMPP como sendo uma tecnologia de mensagens instantâneas e de presença [18] [19].

2.6.1 Arquitectura

O XMPP apresenta uma arquitectura distribuída podendo mesmo existir vários servidores mas nunca existe um servidor central. Por questões de segurança os servidores XMPP podem ser isolados da rede XMPP pública e, ao mesmo tempo, podem existir mecanismos de segurança via canais encriptados, SASL e TLS, descritas nas especificações XMPP Core.
A arquitectura descentralizada tem um comportamento cliente-servidor onde os clientes não comunicam directamente entre si. A figura 2.16 ilustra a organização dos clientes e servidores associados ao protocolo XMPP.

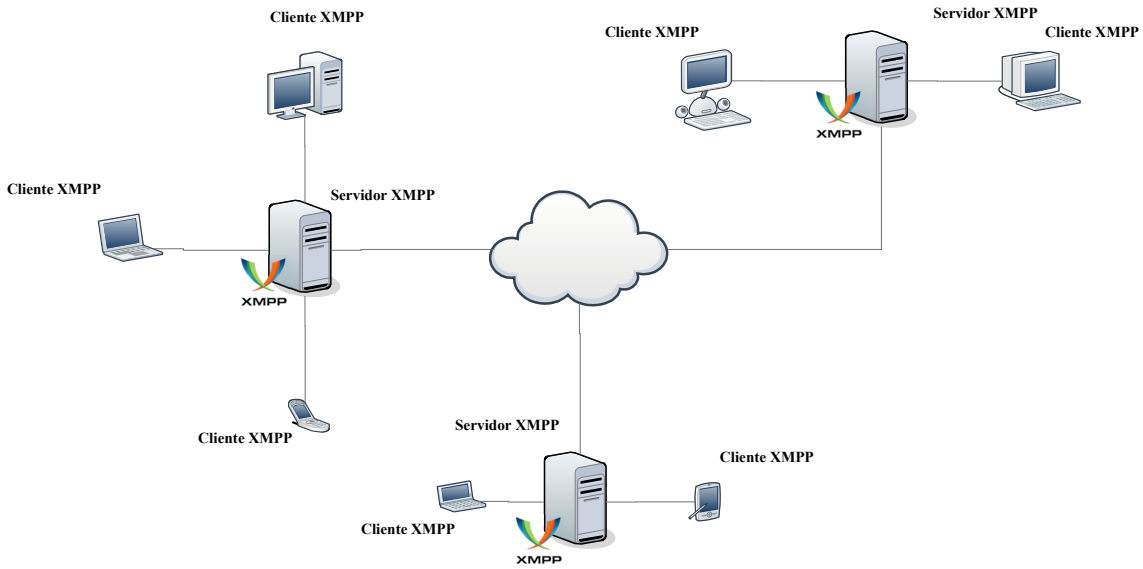


Figura 2.16: Arquitectura distribuída do XMPP

A interligação dos servidores permite que os clientes comuniquem entre si sem estarem, necessariamente, associados ao mesmo servidor.

Stanzas XML

As mensagens XMPP são *Stanzas* XML. Uma *stanza* é uma unidade semântica com informação estruturada, de uma forma especificada pelo contexto, entre duas entidades.
Existem três tipos de de *stanzas* XML definidos para a utilização entre cliente e servidor, *stanzas* do tipo Message, do tipo IQ e do tipo Presence.
As stanzas do tipo **Message** podem ser vistas como um mecanismo de *push*. Uma entidade envia informação para outra à semelhança das comunicações que ocorrem em sistemas como E-mail. Todas as *stanzas* do tipo Message contêm um atributo "to"que especifica o destinatário da mensagem. O servidor ao receber esta mensagem reencaminha-a para o utilizador especificado.
As *stanzas* **IQ** (Info/Query) incorporam um mecanismo do tipo pergunta-resposta. A semântica implementada por este mecanismo permite a uma entidade efectuar um pedido e receber uma resposta de uma entidade sem requerer necessária intervenção directa de um utilizador ou a criação de uma resposta explicita programaticamente. O conteúdo da mensagem é definido na declaração do *namespace* de um elemento *child* directo do elemento IQ e a interacção é assegurada e marcada com recurso ao atributo "id".
Stanzas **Presence** são elementos que podem ser vistas como um mecanismo de *broadcast*. A informação das capacidades de uma entidade é enviada para múltiplos mecanismos que lhe estejam associados/subscritos. Uma entidade que queira publicar o seu *presence* deve enviar a mensagem sem definir o seu atributo "to". A responsabilidade de reencaminhamento destas mensagens é do servidor, que, para cada entidade, verifica as entidades subscritas e encaminha a mensagem para as mesmas. Em determinadas situações uma entidade pode publicar uma stanza presence com o atributo "to"definido, nesse caso o servidor reencaminhará para a entidade especificada como destinatária.

Para os tipos de mensagens previamente descritos existem cinco atributos mais comummente utilizados:

to - Este atributo especifica o destinatário da *stanza*.

from - Atributo que específica o remetente.

id - O atributo "id"é opcional e pode ser utilizado para marcação interna de *stanzas* por forma a controlar o mecanismo pergunta-resposta.

type - Especifica a informação sobre o contexto da *stanza*. Os valores permitidos para este atributo são definidos consoante o tipo de *stanza* em que é utilizado.

xml:lang - Uma *stanza* deve utilizar o atributo "xml:lang"se contiver dados XML que serão apresentados a um utilizador humano. [20]

Servidor XMPP

O servidor XMPP é a entidade que fornece as funcionalidades básicas de troca de pacotes de mensagens, presence, iq e encaminhamento de XML às restantes entidades que comunicam por este protocolo, criando uma camada de abstracção para as comunicações XMPP.
Não existe uma arquitectura de servidor principal. Na rede existem vários servidores XMPP que permitem aos utilizadores comunicar entre si.
Esta entidade é responsável pelo encaminhamento das mensagens de um utilizador para outro mesmo que estejam em servidores diferentes.

O servidor XMPP tem a seu cargo duas funções fundamentais, gerir as conexões/sessões com as entidades através de *streams* XML para/de clientes, servidores ou outras entidades autorizadas e gerir o encaminhamento de *stanzas* XML entre entidades através de *streams* XML [18].

Componente XMPP

Um componente XMPP é uma entidade intermédia situada entre o servidor e o cliente. Esta entidade recebe *stanzas* dos clientes e pode actuar sobre as mesmas, efectuando operações que acomodem a mensagem recebida ou simplesmente a reencaminhem para o servidor.
Conceptualmente um componente XMPP subdivide-se em duas componentes, interna e externa.
A componente **interna** utiliza a API interna do servidor para efectuar as suas operações.
A componente **externa** comunica com o servidor directamente e não está interligada a nenhuma implementação específica de qualquer tipo de servidor.

O protocolo que especifica o comportamento dos componentes define que deve ser utilizada a parte externa de um componente para efectuar a configuração, autenticação e receber/enviar *stanzas* XML através do servidor. [20]
Um componente externo é considerado seguro devido ao tipo de autenticação com o servidor utilizando *shared secret*. Um *shared secret* é normalmente especificado nos ficheiros de configuração do servidor e do componente mas pode ser fornecido em *runtime* por linha de

comandos ou por acesso à base de dados.
Esta parte do componente é encarregue de fazer operações que o cliente não pode/deve efectuar.

Cliente XMPP

A maioria de clientes XMPP utiliza uma ligação por TCP tirando o máximo partido do servidor e dos serviços associados. Um utilizador pode conectar-se ao servidor simultaneamente em vários locais ou dispositivos desde que o cliente esteja autorizado. Para cada local/dispositivo de ligação existe um identificador de recurso que descreve o endereço XMPP (e.g. node@domain/home, node@domain/work). Existe uma porta recomendada para conexões entre o cliente e o servidor registada no IANA como sendo a 5222.

Cada utilizador possui uma identificação que o torna único, denominada Jabber ID (JID). O JID é composto pelos mesmos elementos que um contacto de email, no formato utilizador@domínio (e.g. sensor21@c3s.av.it.pt). Este formato elimina a necessidade de existir um servidor central que possua os dados e informação de todos os JIDs que existem.

A figura 2.17 exemplifica a estrutura de ligação dos vários elementos do protocolo XMPP.

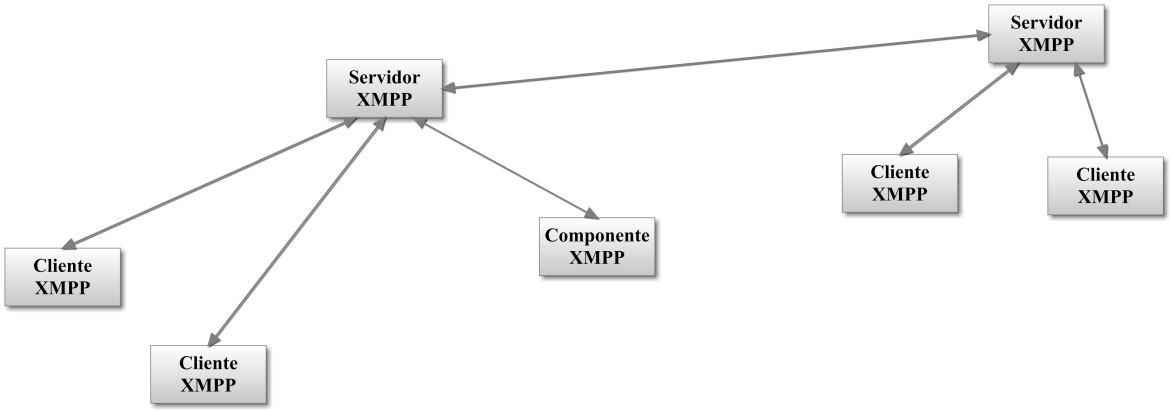


Figura 2.17: Modelo conceptual de funcionamento do XMPP

Extensões

A XMPP *Standards Foundation* desenvolveu extensões para o XMPP através de um processo denominado XMPP Extension Protocols (XEPs). As extensões incorporam no XMPP funcionalidades modulares extra que aumentam a versatilidade do protocolo.
Seguidamente são apresentados algumas extensões relevantes para esta dissertação, *Service Discovery* e PubSub.
O **Service Discovery** é uma extensão que permite a descoberta de informação sobre outras entidades XMPP. Existem dois tipos de informação que podem ser descobertas, a identidade e capacidades da entidade (incluindo os protocolos e funcionalidades que suporta) e os items associados a cada entidade (e.g. *rooms* em que é anfitrião em serviços de *chat* multi-utilizador).
O **PubSub** é uma extensão para utilização do mecanismo publish-subscribe. Esta extensão permite que entidades XMPP criem nós num serviço pubsub e publiquem informação no

mesmo. Por cada actualização da informação num nó é enviada uma notificação de evento para todas as entidades que estejam subscritas no nó. Cada nó pode ser de dois tipos, Collection Node ou Leaf Node. Um **Collection Node** pode conter outros nós agregados a ele próprio mas não pode conter items de publicação. Um **Leaf Node** é um tipo de nó que apenas contém items de publicação. [21]

2.6.2 Implementações

Existem múltiplas implementações dos *standards* XMPP para clientes, componentes e bibliotecas de código, pelo que existe uma vasta gama de aplicações e soluções que recorrem ao XMPP dada a sua flexibilidade na permissão de construção de funcionalidades personalizadas. Além de aplicações XMPP para mensagens instantâneas (IM) existem também aplicações para gestão de rede, publicação de conteúdos, ferramentas de colaboração, troca de ficheiros, jogos e monitorização remota de sistemas.

2.6.3 Fluxo de Mensagens

Quando dois utilizadores querem comunicar entre si fazem-no recorrendo a um servidor, se pertencerem ambos ao mesmo domínio, ou, a dois, se pertencerem a domínios diferentes. A figura 2.18 representa uma troca de mensagens entre dois utilizadores.

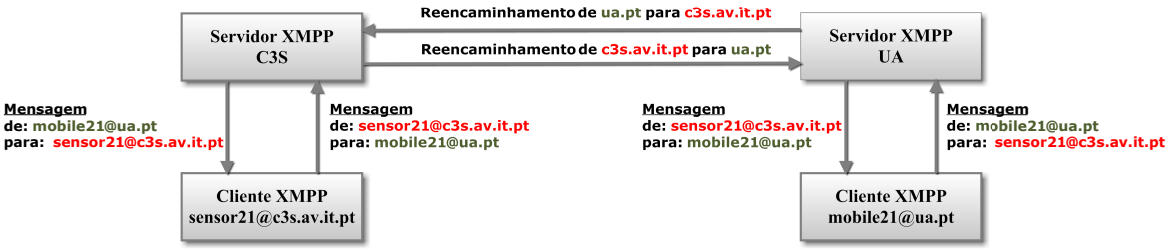


Figura 2.18: Modelo de troca de mensagens XMPP

Exemplifica-se, através da figura 2.18 a uma troca de mensagens entre dois utilizadores. O utilizador sensor21@c3s.av.it.pt envia uma mensagem ao utilizador mobile21@ua.pt que segue o seguinte trajecto. A mensagem é enviada para o seu respectivo servidor, c3s.av.it.pt, aí, será aberta uma ligação para o servidor ua.pt e a mensagem será reencaminhada para este que se encarregará de o enviar ao mobile21@ua.pt. O processo de resposta efectua-se de forma análoga ao envio.

Em situações em que um servidor bloqueia as comunicações com outro, a mensagem é descartada. Noutros casos, se o mobile21@ua.pt quiser comunicar com o sensor21@c3s.av.it.pt e não existirem bloqueios entre servidores, mas o sensor21@c3s.av.it.pt não está conectado, a mensagem é guardada e entregue mais tarde.

2.6.4 Transporte

Uma característica importante do XMPP é a sua capacidade de permitir aos seus utilizadores o acesso a uma rede que possua uma *gateway* XMPP através de protocolos como SMS ou E-mail.
O XMPP permite o acesso ao nível do servidor através da comunicação entre serviços de gateway XMPP em execução num computador remoto. É permitido o registo neste serviço a qualquer tipo de utilizador XMPP desde que forneça as credenciais requeridas. Após registo, o utilizador pode efectuar comunicações com outros utilizadores XMPP da rede. Esta funcionalidade permite a qualquer utilizador aceder a uma rede e comunicar com outros utilizadores XMPP sem estar directamente conectado à Internet e sem necessitar de código extra do lado do cliente, basta para isso que exista uma *gateway* apropriada. [18]

2.7 Síntese de objectivos

Após apresentação dos factores tecnológicos, relembra-se a premissa inicial, a proposta de uma prova de conceito que permita a personalização de aplicações e dispositivos com base na norma 802.21 suportada por uma plataforma de gestão de contexto cuja informação provém de redes de sensores. Reenquadrão-se os objectivos, tirando vantagem da camada 2,5 em que opera o protocolo 802.21 dar-se-á acesso local à informação de contexto gerada pela rede de sensores ao mesmo tempo que se disponibiliza a mesma informação num servidor XMPP (plataforma de gestão de contexto). A utilização deste servidor remoto possibilita não só o armazenamento de dados mas também um acesso alternativo à mesma informação numa plataforma de contexto com teor global.

Capítulo 3

Arquitectura

A solução que se propõe para o problema enunciado centra-se numa arquitectura de implementação que pode ser virtualmente destrinçada numa relação de três componentes já apresentadas, comunicação entre redes heterogéneas demarcada pelo protocolo 802.21, as redes sem fio de sensores e plataformas de gestão de contexto. Esta associação, e consequentes relações, pode ser ilustrada pelo esquema representado na figura 3.1.

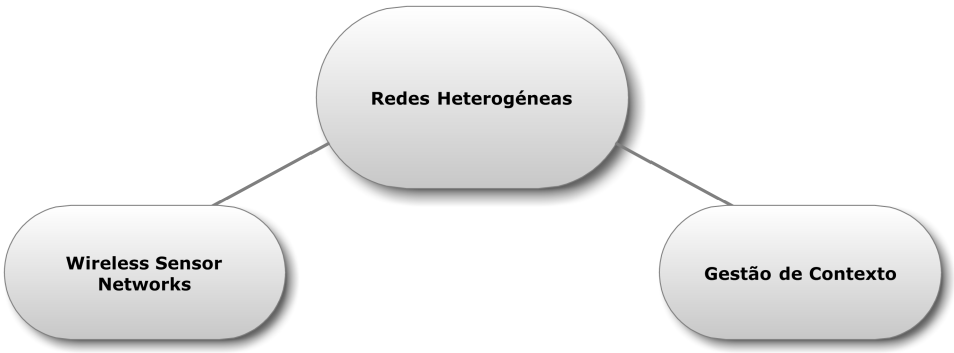


Figura 3.1: Separação Virtual

Identifica-se, na figura anterior, a clara separação de ambientes cuja integração facilita a optimização do funcionamento de redes, equipamentos. aplicações e serviços, através do complemento de partilhada de informação contextual.

3.1 Arquitectura de Serviços

Conceptualmente esta solução implementa o suporte a uma arquitectura de serviços baseada no transporte de contexto entre um utilizador e a fonte de informação através do protocolo MIH da norma 802.21. A arquitectura suporta também, numa situação onde o acesso à informação, usando o protocolo MIH, não está disponível, o sistema publica a informação num servidor de contexto que se encontra disponível para o utilizador, via outro protocolo.

O funcionamento desta arquitectura é demonstrada pela figura 3.2 que reflecte a redundância na possibilidade de acesso à informação através de duas formas distintas.

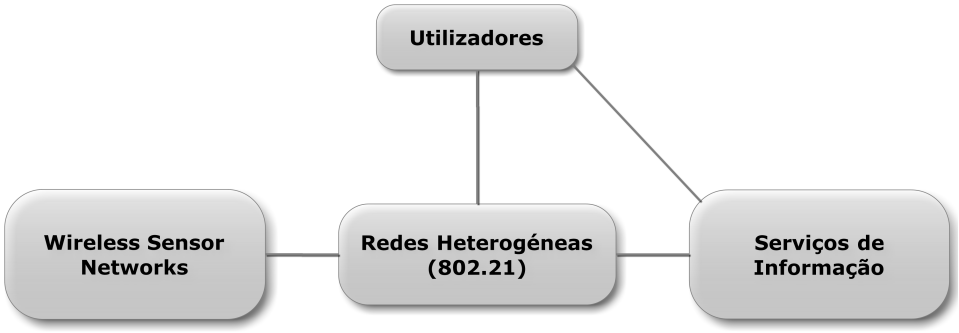


Figura 3.2: Arquitectura de Serviços

3.2 Informação de Contexto

A informação de contexto toma um papel preponderante na construção da camada de inteligência. É através do conteúdo e integração da mesma que se torna possível a avaliação das condições de operação.

Os equipamentos móveis disponíveis no presente já agregam várias formas de recolher informação de contexto, tanto ao nível de *hardware* como *software*, todavia, a quantidade de informação que um dispositivo, em si, produz não é suficiente para avaliar as condições abrangentes com exactidão.

Os sensores vêm introduzir formas para aumentar consideravelmente os meios e medidas para avaliar o contexto envolvente. A grande vastidão de tipos diferentes de sensores contribui para a construção de uma camada de inteligência que permita a tomada de decisões com base na maioria de factores relevantes no contexto.

Associando a informação de contexto aos factores de decisão no suporte a serviços e aplicações obtem-se um mecanismo personalizado e dedicado, à funcionalidade expectável do equipamento, ao contexto em que se encontra e às suas necessidades computacionais. Esta associação requer uma menor interacção do utilizador criando uma camada de abstracção e transparência totalmente funcional e integrada.

3.3 Serviços de Informação

Os serviços de informação facilitam para a rede e aos utilizadores, meios de armazenamento, gestão e disponibilização de informação proveniente de várias entidades e contextos. A implementação, o nível da camada OSI associado à informação que disponibilizam e as formas de dados que gerem, distingue os vários tipos de serviços de informação.

3.3.1 Plataformas de Gestão de Contexto

As plataformas de gestão de contexto, como *context brokers*, permitem às aplicações armazenar a informação e organiza-la de forma a permitir um acesso eficaz e rápido. Este tipo de

serviços de informação disponibiliza mecanismos de acesso à informação que se podem relacionar por histórico e contexto. Baseando-se nestes mecanismos é possível caracterizar e criar uma previsão para certos eventos considerando as condições desejadas e indesejadas tanto ao nível da aplicação como de rede sempre com base em regras e no histórico do contexto.

3.4 Transporte por 802.21

O protocolo MIH 802.21 possui capacidades e potencialidades que permitem o transporte de informação de contexto de uma forma mais generalizada. Para efectuar o transporte de informação de contexto é necessário definir e implementar alguns dos elementos fundamentais que suportam essa comunicação. Na implementação da arquitectura proposta torna-se necessário redefinir os seguintes elementos, o protocolo MIH, MIH Users, MIH Function e MIH SAPs. Esta redefinição na implementação visa a expansão do seu suporte para a informação de contexto orientada a sensores.

Modelo de Componentes MIH

Na arquitectura proposta é necessário a existência de uma *gateway* de sensores com capacidade de comunicação ao nível do protocolo MIH 802.21. Esta *gateway* é composta por dois elementos fundamentais, MIH Function local e por um novo tipo de Link SAP proposto para redes de sensores, o MIH Sensor SAP.

À semelhança do contexto de ligação utilizado nas comunicações *standard* do 802.21, a extensão para sensores suporta também conexões locais e remotas.

As figuras 3.3 e 3.4 representam a arquitectura funcional da *gateway* proposta no modelo de arquitectura com uma abordagem local e remota. Esta dissertação foca-se nos três componentes relevantes para o transporte de contexto representados na figura, MIH User, MIH Function e MIH Sensor SAP.

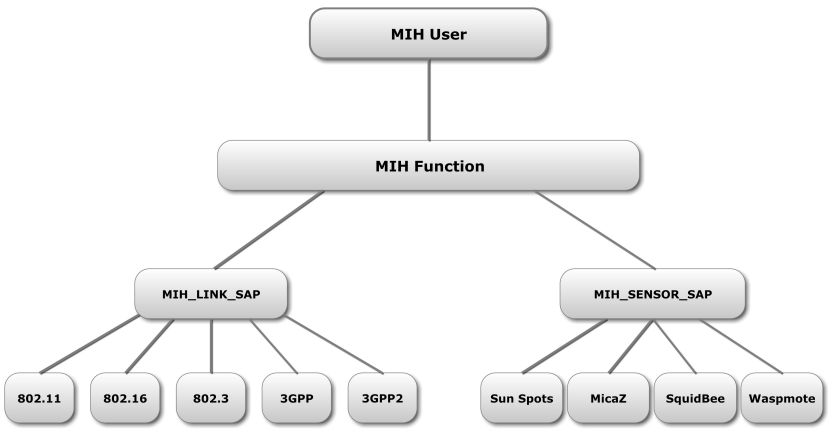


Figura 3.3: Acesso Local

A figura 3.3 representa um modelo de acesso local .

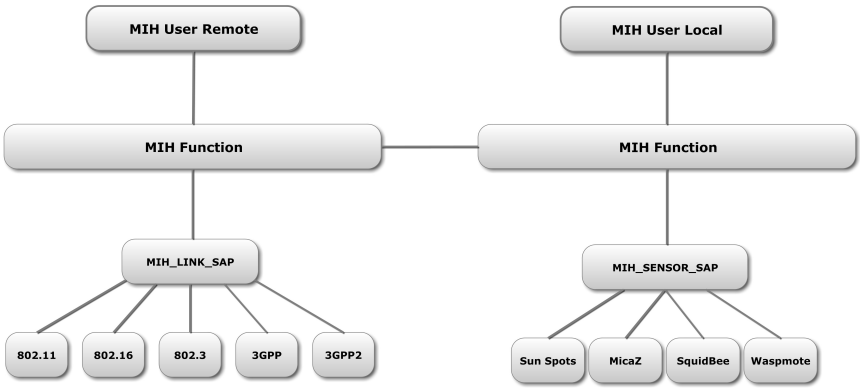


Figura 3.4: Acesso remoto

A figura 3.4 representa um modelo de acesso remoto.

A informação que circula entre sensores e utilizadores é transportada via a extensão para sensores do protocolo MIH 802.21.

3.4.1 Protocolo MIH

A interligação dos elementos necessita da existência, nos elementos da rede, do protocolo MIH que suporte a comunicação.

Como o protocolo MIH da norma 802.21 não foi desenvolvido tendo em vista a inclusão de suporte para informação de contexto torna-se necessário extender este protocolo além do especificado na norma que o acompanha. [1]

A extensão desenvolvida implica a criação de comandos e eventos específicos para sensores, respeitando os mecanismos e regras de parâmetros já utilizadas no protocolo MIH definido pelo IEEE. Apresentam-se, nas secções seguintes, as mensagens, parâmetros e mecanismos implementados, na extensão para sensores, do protocolo MIH.

Mensagens

As mensagens do protocolo MIH são codificadas em formato TLV. Nas tabelas seguintes são apresentadas as mensagens definidas tornando possível a inclusão de informação de sensores. A área a cinzento da tabela representa o cabeçalho do protocolo MIH e as áreas a branco representam os parâmetros que compõem o *payload* da mensagem. O *payload* é composto por um conjunto de parâmetros também codificados no formato TLV.

Uma vez que foi necessário definir novas mensagens, também se tornou necessário definir novos parâmetros e, obrigatoriamente, criaram-se novas entradas nas tabelas de conversão e codificação TLV.

Todas as mensagens têm, no mínimo, dois parâmetros no *payload*, o identificador da fonte (*source identifier*) e o identificador do destinatário (*destination identifier*). Em alguns tipos de mensagens, existem parâmetros opcionais, pelo que não é obrigatória a sua utilização.

Mensagens MIH de Gestão

MIH_Sensor_Capability_Discover.request

Esta mensagem é enviada com o intuito de descobrir as capacidades da rede de sensores relativamente ao protocolo 802.21. Pode ser utilizada em broadcast uma vez que se o utilizador quer descobrir as capacidades da rede há uma grande probabilidade de não saber para que entidades deve enviar a mensagem.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 8)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SupportedMIHSensorEventList (Optional) (MIH event list TLV)
SupportedMIHSensorCommandList (Optional) (MIH command list TLV)
MIHClientSupport (Optional) (MIH client support TLV)

MIH_Sensor_Capability_Discover.response

Esta mensagem é enviada como resposta à mensagem de descoberta de capacidades MIH_Sensor_Capability_Discover.request.

Cabeçalho MIH (SID = 1, Opcode = 2, AID = 8)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SupportedMIHSensorEventList (Optional) (MIH event list TLV)
SupportedMIHSensorCommandList (Optional) (MIH command list TLV)
MIHClientSupport (Optional) (MIH client support TLV)

MIH_Sensor_Event_Subscribe.request

Mensagem utilizada para subscrever eventos MIH de sensores com uma MIHF local ou remota.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
RequestedMIHSensorEventList (Optional) (MIH requested sensor event list TLV)
SensorEventConfigurationInfoList (Optional) (MIH sensor event configuration information list TLV)

MIH_Sensor_Event_Subscribe.response

Mensagem enviada como resposta a MIH_Sensor_Event_Subscribe.request. Indica quais os eventos subscritos com sucesso.

Cabeçalho MIH (SID = 1, Opcode = 2, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
ResponseMIHSensorEventList (Optional) (MIH requested sensor event list TLV)

MIH_Sensor_Event_Unsubscribe.request

Mensagem utilizada para remover a subscrição de eventos MIH.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
RequestedMIHSensorEventList (Optional) (MIH requested sensor event list TLV)

MIH_Sensor_Event_Unsubscribe.response

Mensagem enviada como resposta a MIH_Sensor_Event_Unsubscribe.request e indica quais os eventos dos quais a subscrição foi removida com sucesso.

Cabeçalho MIH (SID = 1, Opcode = 2, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
ResponseMIHSensorEventList (Optional) (MIH requested sensor event list TLV)

Mensagens MIH de Eventos

MIH_Sensor_Event.indication

Mensagem enviada para uma MIHF local ou remota, previamente subscrita, como notificação de um evento despoletado conforme configurado.

Cabeçalho MIH (SID = 1, Opcode = 3, AID = 10)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
MIHSensorParameterReportList (Optional) (MIH sensor parameter report list TLV)

MIH_Sensor_Parameter_Report.indication

Mensagem enviada para uma MIHF local ou remota, como notificação de que um, ou mais, dos limiares configurados foi transpassado.

Cabeçalho MIH (SID = 1, Opcode = 3, AID = 9)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
MIHSensorParameterReportList (Optional) (MIH sensor parameter report list TLV)

Mensagens MIH de Comandos

MIH_Sensor_Configure_Thresholds.request

Mensagem utilizada para configurar limiares de sensores.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
SensorConfigureRequestList (Optional) (MIH requested sensor configuration list TLV)

MIH_Sensor_Configure_Thresholds.response

Mensagem enviada em resposta a MIH_Sensor_Configure_Thresholds.request confirmando a sua configuração.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
SensorConfigureResponseList (Optional) (MIH response sensor configuration list TLV)

MIH_Sensor_Action.request

Mensagem utilizada para a execução local ou remota de acções.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
SensorAction (Optional) (MIH sensor action TLV)
Execution Delay (Optional) (MIH execution delay TLV)

MIH_Sensor_Action.response

Mensagem enviada em resposta a MIH_Sensor_Action.request com resultado da acção executada.

Cabeçalho MIH (SID = 1, Opcode = 1, AID = 6)
Source Identifier = ID MIHF do remetente (Source MIHF ID TLV)
Destination Identifier = ID MIHF do destinatário (Destination MIHF ID TLV)
SensorIdentifier (Optional) (MIH sensor identifier TLV)
SensorAction (Optional) (MIH sensor action TLV)
SensorParameterReportList (Optional) (MIH sensor parameter report list TLV)
SensorDeviceStatesResp (Optional) (MIH response sensor device states list TLV)

Tipos de dados

Para suportar as novas mensagens propostas torna-se necessário propor também novos tipos de dados. Estes novos tipos de dados são orientados ao encapsulamento de informação sensorial. Apenas se apresentam os tipos de dados novos ou alterados, que foram criados tendo em conta a forma com que os dados originais da norma IEEE 802.21 também possuem.

Tipo de Dados	**Derivação**	**Descrição**
MIH_EVT_LIST	BITMAP(32)	Lista de Eventos MIH: Bit de Bitmap: 8: MIH_Sensor_Event 9: MIH_Sensor_Param_Report
MIH_CMD_LIST	BITMAP(32)	Lista de Comandos MIH: Bit de Bitmap: 5: MIH_Sensor_Configure_Thresholds 6: MIH_Sensor_Action
SENSOR_TUPLE_ID	SENSOR_ID	Identificador de um Sensor
SENSOR_ID	SEQUENCE(SENSOR_TYPE, SENSOR_ADDR)	Identificação do sensor composta pelo seu tipo e endereço.
SENSOR_TYPE	UNSIGNED_INT(1)	Representa tipos de Sensores: 0 - Environmental
SENSOR_EVT_CFG_INFO	CHOICE(LIST(SENSOR_CFG_PARAM_PR) LIST(SENSOR_CFG_PARAM))	Informação de configuração.
SENSOR_CFG_PARAM	SEQUENCE(SENSOR_PARAM_TYPE, TH_ACTION, LIST(THRESHOLD))	Utilizado para configurar limiares de operação.
SENSOR_CFG_PARAM_PR	SEQUENCE(SENSOR_PARAM_TYPE, TIMER_INTERVAL, ACTON_EVENT_PR))	Utilizado para configurar notificações periódicas.
SENSOR_PARAM_TYPE	CHOICE(SENSOR_PARAM_LIGHT, SENSOR_PARAM_TEMP, SENSOR_PARAM_ACC)	Tipos de Medidas
ACTION_EVENT_PR	BITMAP(32)	Lista de eventos periódicos disponíveis. Bit de Bitmap:

Continua na próxima página

Tabela 3.1 – Continuado a partir da página anterior

Tipo de Dados	Derivação	Descrição
		0 - MIH_SENSOR_EVENT
SENSOR_ADDR	OCTET_STRING	Endereço MAC
SENSOR_PARAM_LIGHT	UNSIGNED_INT(1)	Tipo de medida 0 - Intensidade Luminosa
SENSOR_PARAM_TEMP	UNSIGNED_INT(1)	Tipo de medida 0 - Temperatura
SENSOR_PARAM_ACC	UNSIGNED_INT(1)	Tipo de medida 0 - Aceleração

Tabela 3.1: Tipos de dados de Mensagens de Gestão de Serviço

Tipos de dados de Eventos

Tipo de Dados	Derivação	Descrição
SENSOR_PARAM_RPT	SEQUENCE(SENSOR_PARAM, CHOICE(NULL, THRESHOLD)	Parâmetros a serem reportados.
SENSOR_PARAM	SEQUENCE(SENSOR_PARAM_TYPE, SENSOR_PARAM_VAL)	Par (Tipo, Valor) para cada tipo de sensor.
SENSOR_PARAM_VAL	INTEGER(2)	Valor actual medido pelo sensor

Tabela 3.2: Tabela de tipos de dados de eventos

Tipos de dados de Comandos

Tipo de Dados	Derivação	Descrição
SENSOR_STATUS	UNSIGNED_INT(1)	Estado da basestation: 0 - UP, 1 - Down.
SENSOR_AC_TYPE	UNSIGNED_INT(1)	Especificação da acção a ser executada: 0 - Desconectar 1 - Power Down 2 - Power UP 3 - Sensor ReadOut
Continua na próxima página		

Tabela 3.3 – Continuado a partir da página anterior

Tipo de Dados	Derivação	Descrição
CONFIG_STATUS	LIST(BOOLEAN)	Status da configuração: TRUE - sucesso, FALSE - erro.
DEV_SENSOR_STATES_RSP	SEQUENCE(DEVICE_INFO, BATT_LEVEL, SENSOR_STATUS,)	Estado de funcionamento da basesation.
SENSOR_CFG_STATUS	SEQUENCE(SENSOR_PARAM_TYPE, THRESHOLD, CONFIG_STATUS,)	Status de configuração para cada parâmetro de limiar configurado.
DEVICE_INFO	OCTET_STRING	Endereço MAC da basestation.
BATT_LEVEL	INTEGER(1)	Estado da bateria: [-1 , 100] -1 = Desconhecido; 100 = Máximo

Tabela 3.3: Tabela de tipos de dados de comandos

Valores para codificação TLV de sensores

O standard IEEE MIH 802.21 define valores para os tipos de dados TLV especificados no standard com numeração entre 1 e 63 e define ainda que existe uma gama reservada de TLVs com numeração de 64 a 99. É nesta gama reservada que se definiram os valores TLV para as novas mensagens de extensão para sensores do protocolo MIH 802.21.

Nome do Tipo de TLV	Valor do Tipo de TLV	Tipo de Dados
SensorIdentifier	64	SENSOR_TUPLE_ID
RequestedMIHSensorEventList	65	MIH_EVT_LIST
SensorEvtConfigInfoList	66	LIST(SENSOR_EVT_CFG_INFO
SensorParameterReportList	67	LIST(SENSOR_PARAM_RPT)
SensorIdentifierList	68	LIST(SENSOR_TUPLE_ID)
SensorDeviceStatesResponse	69	DEV_SENSOR_STATES_RSP
SensorConfigureRequestList	70	LIST(SENSOR_CFG_PARAM)
Continua na próxima página		

Tabela 3.4 – Continuado a partir da página anterior

Nome do Tipo de TLV	Valor do Tipo de TLV	Tipo de Dados
SensorConfigureResponseList	71	LIST(SENSOR_CFG_STATUS)
SensorAction	72	SENSOR_AC_TYPE
ExecutionDelay	73	LIST(SENSOR_CFG_STATUS)
SensorSupport	74	SENSOR_AC_TYPE

Tabela 3.4: Tabela de valores para codificação TLV

3.4.2 MIH_Users

Neste tipo de arquitectura orientada à informação de contexto, os MIH Users são quem faz uso da informação. Os MIH Users utilizam as mensagens específicas do protocolo MIH orientado a sensores para obter e controlar a informação dos sensores bem como, em algumas situações, o seu funcionamento. Os dados obtidos permitirão efectuar e afectar a tomada de decisões ao nível do *handover* ou ao nível da aplicação.

A informação recolhida deve ser processada e comparada, com algum tipo de métrica seleccionada, para afectação de decisões.

Apresenta-se uma proposta de arquitectura do tipo acção/reacção baseada em informação de sensores. Este modelo subdivide-se em quatro elementos de actividades, Comunicação 802.21, Recolha de Dados, Avaliação e Acção e estão representados no diagrama de actividades ilustrado na figura 3.5.

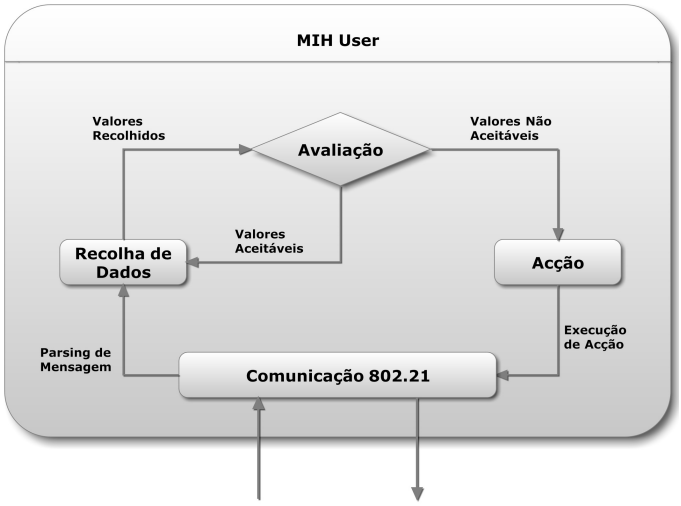


Figura 3.5: Diagrama de Actividades dos MIH Users

No seguimento da recepção de mensagens relativas à informação de sensores o módulo de Comunicação 802.21 faz o *parsing* da mensagem e envia os dados recolhidos relevantes para o contexto para o modelo de Recolha de dados, que os processa e disponibiliza internamente para outros processos. Seguidamente o processo de Avaliação decide, perante os dados actualizados no modelo de Recolha de Dados, a validade dos mesmos perante as suas necessidades de execução e tomará uma acção se não se satisfizerem os requisitos ou continuará a processar os dados que vai recolhendo.

3.4.3 MIH Sensor SAPs

É através de módulos de comunicação tecnologicamente específicos que a informação de sensores é obtida e disponibilizada pelo protocolo MIH 802.21. Por este motivo é proposta uma arquitectura para implementação de SAPs específicos para sensores, MIH Sensor SAPs.

Em situações previstas pelo standard são utilizados os módulos MIH Link SAP para a comunicação directa e específica com os vários meios físicos de comunicação e respectivas tecnologias (e.g. 802.11, 802.16, 802.3, etc.). Na abordagem à extensão para sensores proposta é utilizado um MIH Sensor SAP, com um funcionamento análogo ao já descrito MIH Link SAP, para obter dados e valores sensoriais e disponibilizar os mesmos via protocolo MIH 802.21.

A figura 3.6 representa o diagrama de actividades necessário para o funcionamento desde módulo e é composto por quatro elementos de actividades, a Comunicação 802.21, o Armazenamento Local, a Recolha de Dados e a Acção sobre Sensores.

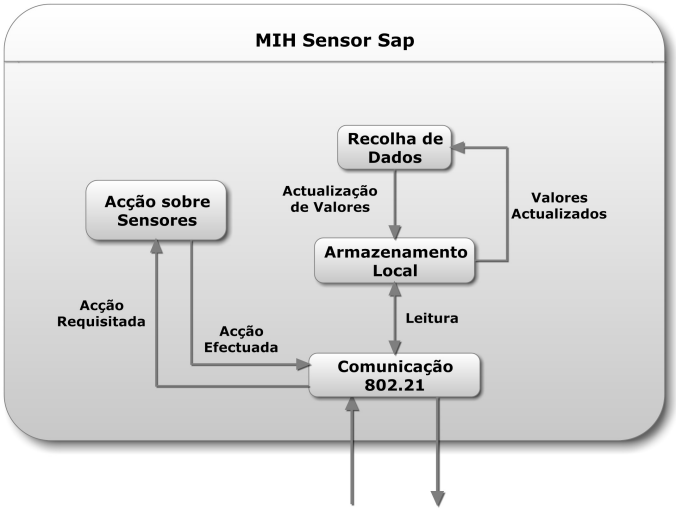


Figura 3.6: Diagrama de Actividades de Sensor SAPS

Neste diagrama de actividades existe um módulo de **Recolha de Dados** que se dedica à constante obtenção de dados de sensores e a sua validação uma vez que por vezes podem ser recolhidos valores irrelevantes derivado a erros na rede ou mau funcionamento dos

dispositivos. Este módulo assim que valida os valores obtidos envia-os para o processo de **Armazenamento local** que armazena localmente informação sensorial e dados de dispositivos (sensores) associados, permitindo uma disponibilização mais rápida da informação. Este mecanismo evita que se efectue uma pergunta/resposta aos sensores cada vez que a informação for requerida, evitando sobrecarga na rede e diminuindo o tempo de execução.
Cada vez que o módulo **Comunicação 802.21** recebe um pedido acede ao módulo de Armazenamento Local e faz uma leitura dos campos que lhe foram requeridos. Eventualmente, podem ser emitidas ordens de acção aos sensores, nestas situações, esta responsabilidade é delegada para o módulo de **Acção sobre Sensores** que cumprirá as suas funções perante os sensores e devolverá uma resposta com o resultado.

3.4.4 MIHF

A MIH Function é o elemento central nesta arquitectura, é através deste elemento que as mensagens são encaminhadas entre os MIH Users e os vários SAPs.

A expansão para sensores tem implicações directas no funcionamento da MIHF a dois níveis, no reconhecimento de mensagens e no suporte à especificação de serviços. A figura 3.7 ilustra a expansão dos vários elementos internos à MIHF para permitir o suporte a sensores.

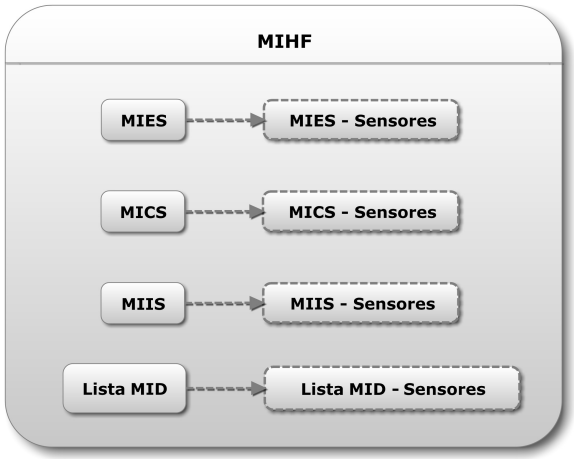


Figura 3.7: Expansão para sensores e suporte da MIHF

Os serviços existentes, bem como os mecanismos associados, como já referido, não suportam, por base, as mensagens de sensores concebidas, por este motivo, tendo sido necessário a definição de mensagens MIH 802.21 orientadas exclusivamente aos sensores torna-se necessário a **expansão dos serviços de eventos, comandos e de informação**. O suporte a estas novas mensagens é conseguido através da inclusão dos serviços expandidos nos mecanismos previamente existentes e definidos pelo *standard*. A interacção das novas mensagens com os mecanismos de suporte já existentes deve ser transparente uma vez que os moldes das mensagens criadas são baseados nas definições estipuladas pelo protocolo 802.21

Ao nível do **reconhecimento de mensagens**, o standard 802.21 MIH *Services* específica que qualquer mensagem cujo identificador não seja reconhecido é descartado à partida. Para que as mensagens de sensores, uma vez que foram criadas de raíz e não são contempladas originalmente pelo *standard*, não sejam descartadas é necessário expandir a lista de identificadores de mensagem (MID), incluindo todas as mensagens criadas para o transporte de informação de contexto sensorial.

3.5 Gestão de Endereços IP

Uma das questões que se colocam com o aumento exacerbado dos dispositivos sensoriais é a gestão de endereços IP. Presentemente o IPv4 começa a escacear dado o elevado número de equipamentos a nível mundial que utiliza este tipo de endereço e mesmo o facto do IPv6 ser mais abrangente no número de endereços disponíveis, ao ritmo que a tecnologia de sensores evolui, rapidamente se deparará com o mesmo problema. Se todos os sensores utilizarem um endereço IP claramente a *pool* de endereços estará esgotada com relativa facilidade.

A extensão para sensores do protocolo MIH 802.21 tira partido do facto deste protocolo se colocar numa camada intermédia L2,5 uma vez que permite aos sensores comunicarem os seus dados e estarem disponíveis para a rede sem necessitarem de obter ligação L3, e consequentemente, não utilizam um IP da *poo* de endereços. Se os dispositivos sensoriais não necessitarem de IP este protocolo beneficiará os mecanismos de atribuição de IP bem como os processos de *handover* baseados em informação de contexto.

3.6 Transporte alternativo

A utilização de um meio de transporte alternativo nesta arquitectura providencia um mecanismo de redundância na obtenção da informação de contexto.

Na arquitectura proposta existem dois componentes fundamentais e distintos suportados pelo transporte alternativo numa distribuição de entidades com a integração apresentada, o elemento que está associado à rede constantemente e utiliza a comunicação via 802.21 para aceder à informação de contexto publicando a mesma para um servidor de informação e um elemento móvel que faz uso da informação disponibilizada no servidor de informação quando a comunicação via 802.21 não está disponível.

A figura 3.8 representa o modelo de transporte alternativo acima descrito. Existe um utilizador, na figura representado pelo Utilizador 1, que coloca a informação num servidor que providencia serviços de informação e um utilizador, na figura representado pelo Utilizador 2, que descobre a localização do servidor através do protocolo 802.21 com a rede em questão e depois efectua o acesso à informação de contexto através deste servidor. A disponibilização e acesso à informação no servidor pode ser efectuado através de outro protocolo conhecido (e.g. HTTP, XMPP, *etc.*) que dependerá da implementação utilizada.

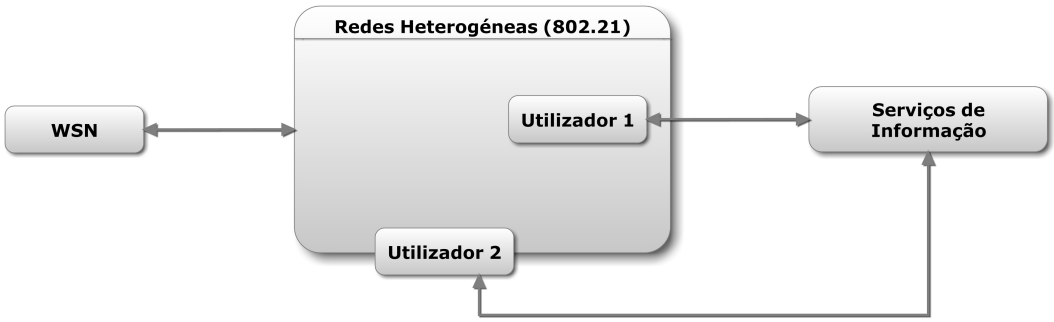


Figura 3.8: Transporte alternativo

3.6.1 Mecanismo de Disponibilização

Para implementar o mecanismo de transporte alternativo previamente descrito propõe-se que a troca de informação entre estes três elementos (entidade que disponibiliza os dados, entidade que acede os dados e servidor) seja efectuada com base num modelo Publicador/-Subscritor.

A figura 3.9 ilustra a organização do modelo Publicador/Subscritor em três entidades distintas, publicador, servidor e subscritor.

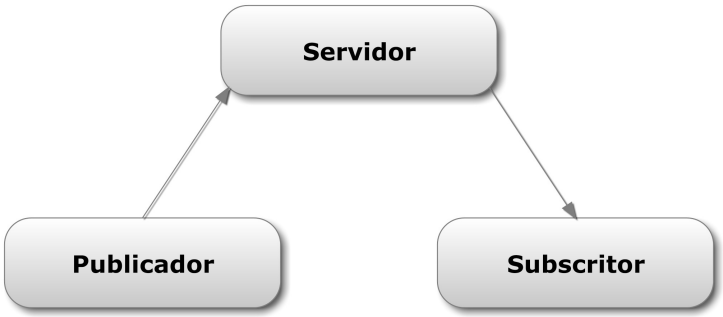


Figura 3.9: Modelo Publicador/Subscritor

Publicador

O elemento publicador é responsável pela disponibilização e publicação para o servidor (serviços de informação) da informação de contexto reunida pela extensão para sensores do protocolo MIH 802.21.

Subscritor

O elemento subscritor acede ao servidor, subscrevendo os serviços nos quais está interessado e recebe as actualizações da informação subscrita.

Servidor

O servidor disponibiliza os mecanismos que permitem o suporte a publicadores e subscritores. Encarrega-se da organização e estruturação dos dados recebidos bem como a distribuição dos conteúdos para os utilizadores subscritos.

Nesta arquitectura de publicador/subscritor, sempre que a informação for actualizada pelo publicador deve ser imediatamente distribuída pelos subscritores associados ao mesmo tempo que é incluída no seu histórico e colocada na cache de eventos recentes. Esta arquitectura é importante uma vez que evita a necessidade de consultas constantes por parte do utilizador (subscritor). Com este mecanismo o utilizador tem a garantia que assim que houver uma actualização de informação esses dados serão automaticamente reencaminhados para os subscritores.

Capítulo 4

Implementação

4.1 Protótipo

Foi desenvolvido um protótipo que visa a disponibilização de acesso a informação de contexto aos utilizadores de uma rede através do protocolo 802.21 que em conjunto com o protocolo XMPP criam uma forma de redundância no acesso à informação e potenciam uma framework para procedimentos de *handover* baseados em informação de contexto e serviços de alto nível personalizados.

Para um utilizador móvel a deslocação é um factor constante, por este motivo estima-se que ao longo do seu movimento vá encontrando novas redes e novas formas de ligação, e uma vez que cada utilizador tem necessidades específicas e cada rede produz informação diferente, torna-se extremamente importante a forma como é gerida a ligação com a rede.

Ao entrar no alcance de ligação de uma rede o utilizador não conhece as potencialidades da rede à qual se vai ligar, por este motivo, todas as funcionalidades de uma rede são-lhe transparentes e as suas necessidades não podem ser expressas. Para que estas situações sejam minimizadas e as potencialidades de uma rede sejam aproveitadas, o protótipo demonstra formas de descobrir as capacidades da rede e os mecanismos de acesso às mesmas.

O protótipo implementa três mecanismos base, o mecanismo de descoberta através do qual um utilizador fica a conhecer as potencialidades da rede, o mecanismo de acesso às potencialidades e informação providenciada pela rede, e o mecanismo através do qual esta informação é disponibilizada.

4.2 Arquitectura da Implementação

A arquitectura implementada no protótipo assenta num modelo de distribuição de informação sustentada no protocolo 802.21, cuja versão *open source* provém do projecto ODTONE, e disponibilização dos dados recolhidos referentes a informação de contexto num servidor XMPP, pertencente ao projecto PT *Context Broker*. Adicionalmente existe a possibilidade de consulta de informação através do *website* Pachube (ver Anexo D) que disponibiliza uma versão do Google Maps onde se torna fácil de localizar os sensores alvo, sendo possível, a partir dessa localização, aceder aos dados publicados. A figura 4.1 ilustra a arquitectura

implementada através dos seus blocos de componentes.

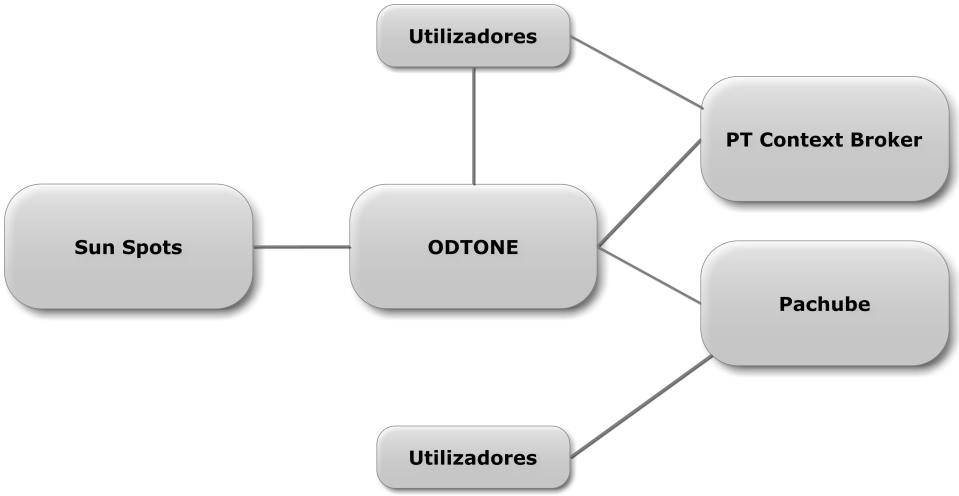


Figura 4.1: Arquitectura de Serviços

4.2.1 Comparação de Arquitecturas

Analisando a arquitectura implementada, representada pela figura 4.1 e a arquitectura proposta para sistemas com esta configuração pode-se inferir que a organização da implementação obedece aos estruturação dos blocos conceptuais apresentados na arquitectura proposta.

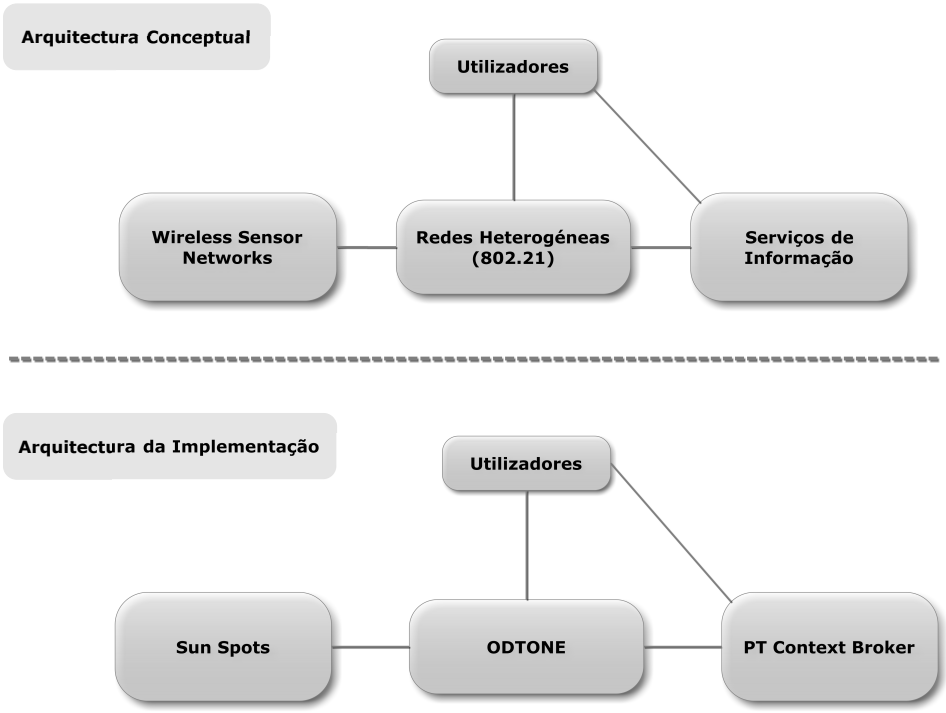


Figura 4.2: Arquitectura de Serviços

4.3 Concepção da Implementação

O desenvolvimento da prova de conceito envolveu dois passos fundamentais na construção da infra-estrutura que se apresenta. Estes passos revelam o trabalho efectuado na área da programação relativa à implementação.

O primeiro passo da concepção da implementação foi a implementação em Java do protocolo MIH 802.21 seguido da extensão para sensores das mensagens protocolares e dos mecanismos que se fazem acompanhar. Seguidamente criaram-se rotinas de funcionamento para os Sun Spots e a respectiva rede de sensores, neste passo foi necessário gerir e avaliar a informação que se recebia dos dispositivos para que não fossem injectados na rede dados incoerentes.

Num segundo passo criaram-se as três entidades que acompanham a prova de conceito (ver 4.4), a *gateway* 802.21 da rede de sensores, o utilizador móvel e o utilizador publicador. Ainda neste passo implementou-se os procedimentos de estabelecimento de comunicações tanto ao nível do protocolo 802.21 como XMPP. Foi necessário implementar os MIH Users, o *Context Consumer*, o *Context Provider* e o Pachube *Publisher*, respectivamente aos protocolos que utilizam e de acordo com as especificações referidas na arquitectura proposta (ver 4.2).

4.4 Prova de Conceito

Como prova de conceito, este protótipo foi instalado numa *testbed* e usaram-se cenários seleccionados para demonstração das potencialidades da integração das três áreas tecnológicas já referidas.

Para a construção da *testbed* que envolve o protótipo foram utilizados três computadores, um deskop, um laptop e um netbook, representando entidades activas na rede. Foi utilizado também um *kit* de Sun Spots composto por dois dispositivos Sun Spot e uma basestation. Para armazenamento e distribuição de informação foram utilizados um servidor XMPP, PT Context Broker, e um Web Service dedicado a informação sensorial, Pachube.

Os Sun Spots fornecem uma fonte de informação composta por uma rede sem fio de sensores de nós individuais sem comunicação entre pares. A informação sensorial de cada nó é recolhida por uma *basestation* que faz a gestão e validação das medidas recebidas. A informação reunida pelos Sun Spots e *basestation* é organizada numa *gateway* responsável pela disponibilização dos dados para o transporte por 802.21.

A figura 4.3 representa a *testbed* construida em laboratório bem como as interacções entre os vários elementos. A legenda embutida na figura especifica os protocolos utilizados nas interacções. A ligação entre os três computadores presentes no cenário da figura foi conseguida através de Ethernet numa LAN com acesso à internet.

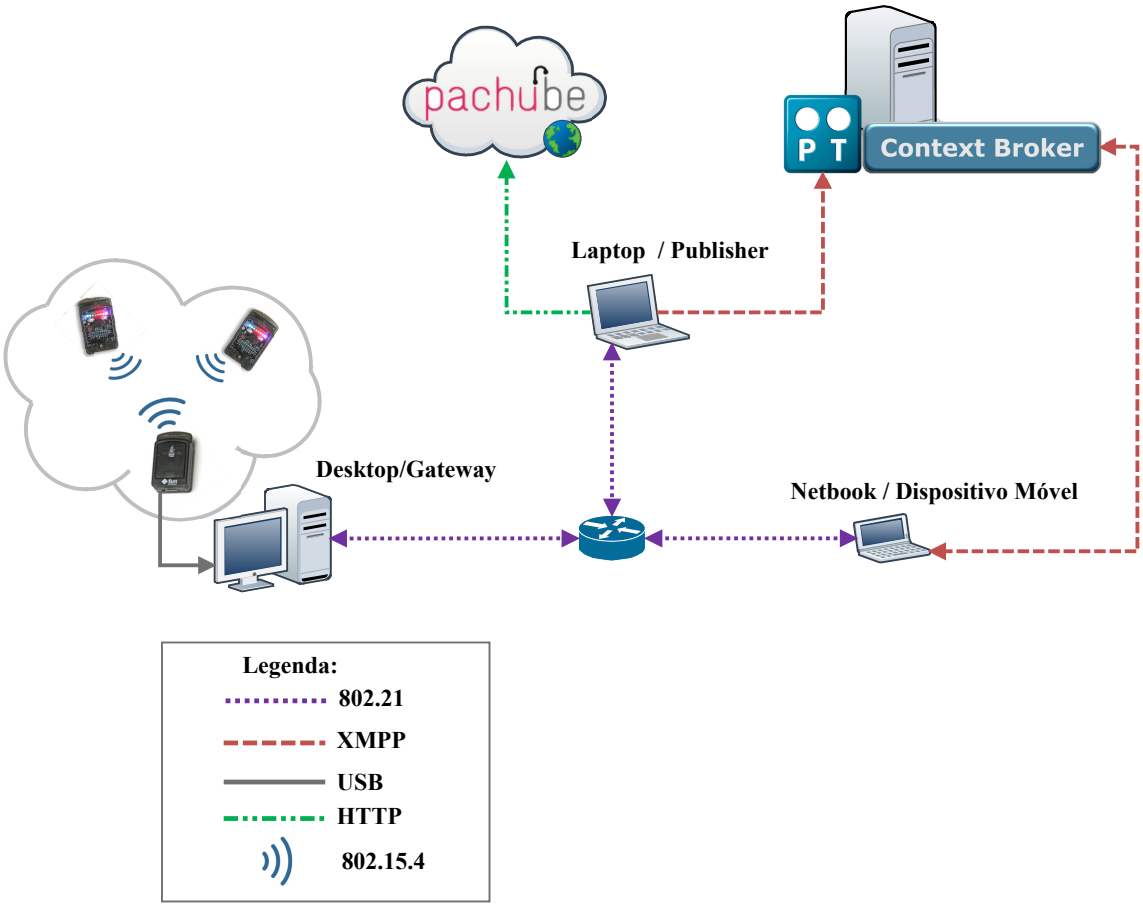


Figura 4.3: Cenário de testes

O protótipo implementa quatro mecanismos base, o mecanismo de descoberta através do qual um utilizador fica a conhecer as potencialidades da rede, o mecanismo de configuração e subscrição de eventos, o mecanismo de publicação/disponibilização de informação e o mecanismo de consumo de informação.

O funcionamento destes mecanismos é demonstrado com recurso a cenários de teste utilizando os dois meios de acesso a informação disponíveis.

4.5 Cenários

Para testar a prova de conceito elaborada foram elaborados dois cenários hipotéticos para demonstração do funcionamento do protótipo.

A diferença nos cenários centra-se no mecanismo de acesso à informação utilizado pelo utilizador móvel. A figura 4.4 é uma fotografia da *testbed* utilizada realçando as entidades intervenientes nos cenários.

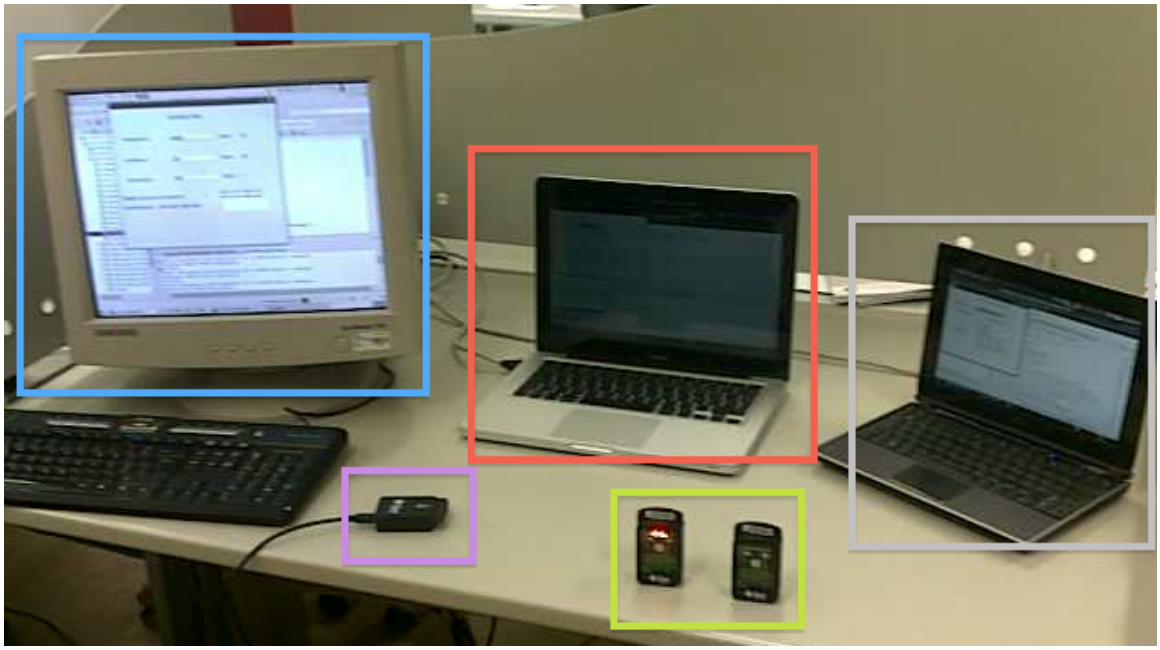


Figura 4.4: Fotografia da Testbed

Na imagem podem ser visualizados dois tipos de elementos, os computadores, e os nós da rede de sensores. Os computadores são compostos por, mais à esquerda, a *gateway* dos sensores (Desktop) onde se encontra a MIHF1 e a MIH Sensor SAP, no centro, o equipamento do utilizador publicador (laptop) com a MIHF2 e o MIH User correspondente e o último computador, o utilizador móvel (Netbook) composto pela MIHF3 e o MIH User respectivo. Os sensores compõe se por 2 tipos de nós, dois dispositivos Sun Spots (à direita) que são compostos por vários sensores e são a entidade que recolhe os dados sensoriais, e a Basestation (à esquerda) que recebe a informação dos dispositivos Sun Spots agregando-a e disponibilizando-a para a MIH Sensor SAP.

4.5.1 Cenário 1 - Acesso Directo

Neste cenário o utilizador móvel acede à informação de contexto directamente pela rede onde está associado utilizando as mensagens de protocolo 802.21. A figura 4.5 representa as ligações utilizadas e o trajecto existente das comunicações no cenário onde é abordado um acesso directo à informação.

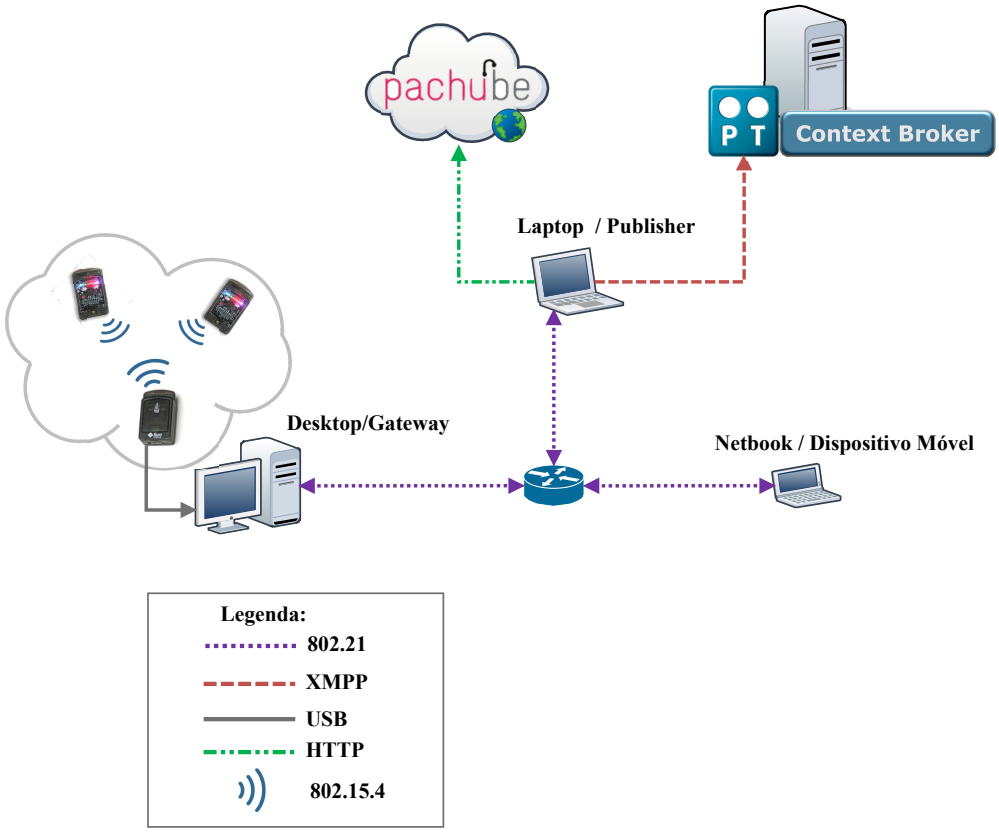


Figura 4.5: Acesso directo à informação de contexto por 802.21

Na resposta à mensagem de descoberta de capacidades, além de o utilizador ser informado do suporte ao acesso directo à informação pela *gateway* 802.21 num dos parâmetros da mensagem de resposta é também encapsulado, na forma de listas, os comandos e eventos suportados.

Num passo seguinte, o utilizador envia uma mensagem à *gateway* subscrevendo os eventos e comandos que deseja utilizar e dos quais quer receber uma notificação, especificando também uma periodicidade para essas notificações. Após a mensagem de subscrição ser enviada é retornada uma resposta que indica o sucesso ou insucesso do processo de subscrição. Se a subscrição for bem sucedida, o utilizador passará a receber notificações, sobre os eventos que subscreveu, com a periodicidade que explicitou previamente.

Eventualmente, e dependendo do utilizador, pode ser utilizado um mecanismo implementado baseado em Pergunta/Resposta através de um comando denominado MIH Sensor Action. Este comando permite ao utilizador executar remotamente uma acção, nesta situação, é oferecida ao utilizador a hipotese de pedir ao *gateway* que faça um "*read out*"aos sensores, devolvendo o estado/medidas dos sensores.

4.5.2 Cenário 2 - Acesso Indirecto

Para este cenário, o utilizador móvel utiliza um servidor XMPP remoto para aceder à informação de contexto uma vez que a rede não lhe oferece suporte directo através de mensagens de protocolo 802.2. A figura 4.6 representa as ligações utilizadas e o trajecto existente das comunicações no cenário onde é abordado um acesso indirecto à informação.

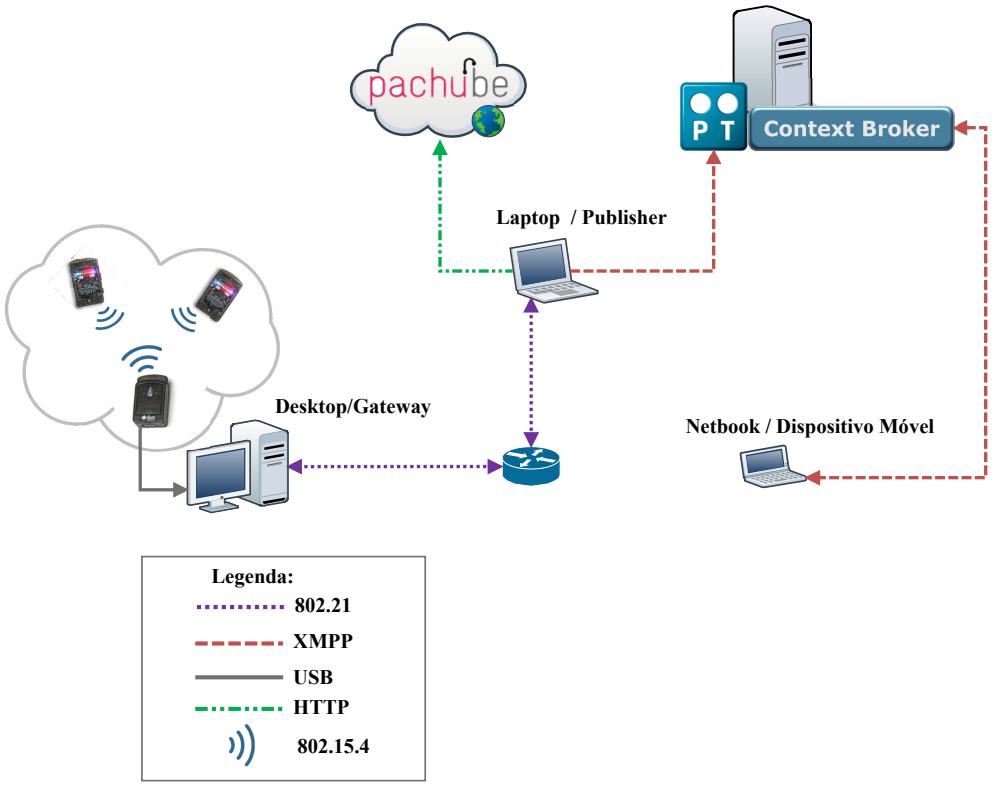


Figura 4.6: Acesso indirecto à informação de contexto por 802.21

Quando a *gateway* 802.21 apenas suporta o acesso indirecto, na resposta à mensagem de descoberta de capacidades é encapsulado um parâmetro que indica o endereço de um servidor XMPP e o nó a que o utilizador se deve subscrever para receber informação de contexto produzida pela rede de sensores. Neste caso, o servidor é o PT Context Broker e o utilizador após receber o seu endereço envia uma mensagem XMPP com o mecanismo PubSub que permite a subscrição de um dado nó. Se a subscrição for bem sucedida serão enviadas, ao utilizador, notificações aquando da actualização da informação. A forma como a informação é colocada no PT Context Broker é transparente para o utilizador móvel.

4.6 Mecanismos e Processos

O funcionamento das duas entidades que representam os utilizadores obedece a uma ordem de operações representada pela figura 4.7 onde são representados os quatro mecanismos conceptuais implementados.

Figura 4.7: Ordem de Funcionamento dos Mecanismos dos Utilizadores

Os utilizadores começam por aceder à rede por 802.21 e accionam o mecanismo de **Descoberta** para ficarem cientes das capacidades da rede em termos de contexto. Após o mecanismo de descoberta estar completo e mediante o meio de acesso disponível (802.21 ou XMPP) accionam o mecanismo de **Subscrição/Configuração** que mediante o protocolo subscreve e/ou configura regras para a recepção informação. Após estes mecanismos estarem concluídos procede-se ao consumo da informação através do mecanismo de **Consumo** onde a informação é recolhida e tratada programaticamente. Se a informação estiver a ser consumida por 802.21 é possível questionar quanto ao mecanismo de publicação/disponibilização, se o utilizador for publicador utiliza ainda um mecanismo de **Disponibilização** que lhe permite publicar a informação no servidor XMPP do PT Context Broker. Se a informação estiver a ser consumida por XMPP através do PT Context Broker ou o utilizador não estiver programado para publicar a informação então a publicação não ocorre e a informação serve apenas para utilização interna do mecanismo de consumo.

4.6.1 Descoberta

No mecanismo de Descoberta, o utilizador obtém ligação ao nível L3 por Ethernet com a rede e envia uma mensagem, por Broadcast e utilizando o protocolo 802.21, requisitando informação sobre as capacidades suportadas pela rede. A este pedido de descoberta de capacidades apenas é considerada a resposta da *gateway* 802.21 da rede de sensores, representada pelo desktop, que responde com as capacidades de contexto e respectivos meios de acesso a informação que suporta. A partir deste processo de descoberta existem dois cenários possíveis. No primeiro cenário, existe um suporte completo para acesso à informação de contexto através de mensagens de protocolo 802.21. No segundo cenário, a *gateway* informa ao utilizador que, por algum motivo, não existe suporte directo disponível através de mensagens de protocolo

802.21 e encapsula, na mesma mensagem, o endereço de um servidor XMPP bem como o nó onde a informação de que possui está a ser disponibilizada a à qual pode aceder através do mecanismo PubSub do protocolo XMPP (mensagens XMPP encontram-se no anexo E.

As figuras 4.8 e 4.9 representam os diagramas de sequência implementados para a troca de mensagens efectuada pelo mecanismo de descoberta de capacidades dos utilizadores Móvel e Publicador.

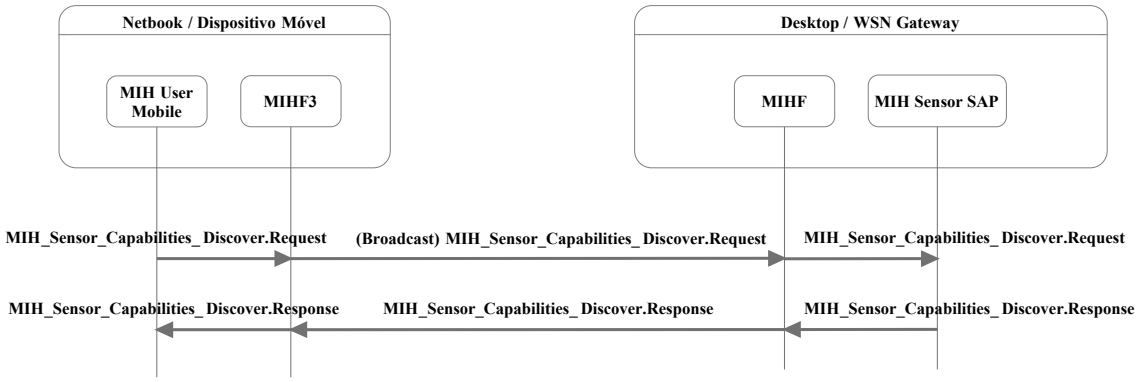


Figura 4.8: Mecanismo de Descoberta accionado pelo MIH User do Utilizador Móvel

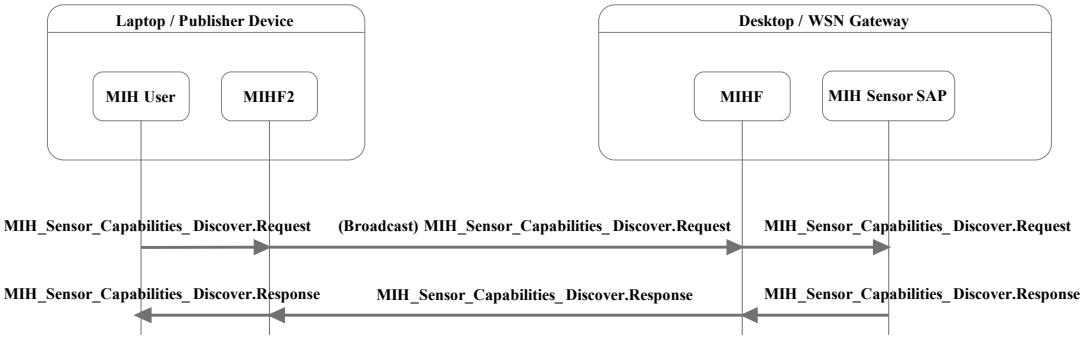


Figura 4.9: Mecanismo de Descoberta accionado pelo MIH User do Utilizador Publicador

Tal como descrito no mecanismo de Descoberta podem ser analisados os dois diagramas analogamente. O MIH User envia a mensagem **MIH Sensor Capabilities Discover.request** por Broadcast e é lhe respondido pelo MIH Sensor SAP com uma mensagem **MIH Sensor Capabilities Discover.response** indicando os tipo de acesso à informação de contexto suportados (802.21 ou XMPP) bem como eventos e comandos disponíveis.

4.6.2 Meios de Acesso à Informação

O suporte para acesso à informação é anunciado aquando da descoberta de capacidades ao utilizador móvel e pode-se processar por duas formas. Directamente, utilizando mensagens de protocolo 802.21 ou, indirectamente, através de XMPP acedendo a um servidor remoto. Este mecanismo permite que a rede delegue as funções implementadas pelo protocolo 802.21

ao nível de suporte de informação de contexto para outras redes ou protocolos, auxiliando a gestão de recursos.

4.6.3 Subscrição e Configuração de Eventos

Independentemente da escolha de protocolo utilizado, é necessária uma subscrição e/ou configuração de regras para recepção e consumo da informação de contexto.

Subscrição por XMPP

No caso do transporte de contexto por XMPP, o utilizador subscreve um nó num endereço de um servidor através do mecanismo PubSub do protocolo XMPP. A informação sobre o nó e o endereço do servidor é obtida pela mensagem de resposta no processo de descoberta de capacidades. Existem dois tipos de subscrição, para o utilizador móvel e para o utilizador publicador.

Para o *Context Consumer* do utilizador móvel, a subscrição passa pelo envio de uma mensagem de XMPP para o PT Context Broker (servidor XMPP) indicando o nó a que pretende subscrever. A figura 4.10 ilustra o diagrama de sequência da troca de mensagens de subscrição XMPP entre o utilizador móvel e o PT Context Broker.

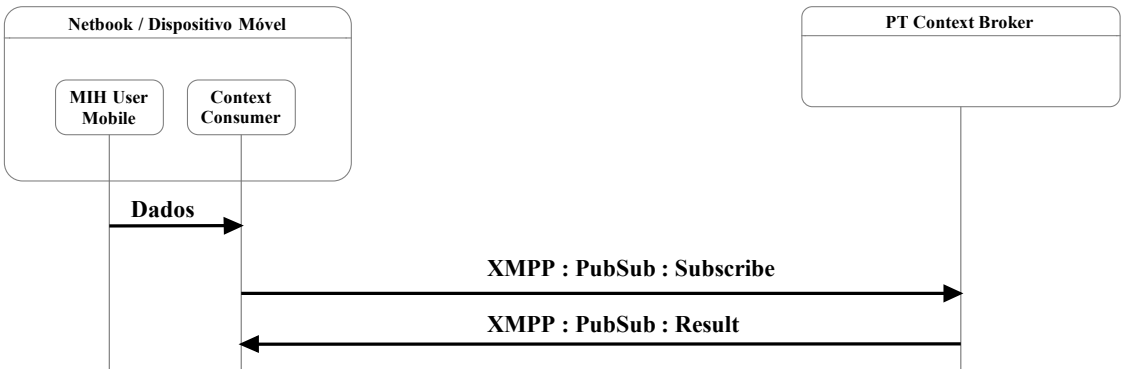


Figura 4.10: Mecanismo de Subscrição/Configuração accionado pelo Context Consumer do Utilizador Móvel

Para o*Context Provider* do utilizador publicador, a subscrição não é mais que uma ligação ao servidor através das APIs utilizadas para permitir a publicação directa para o nó especificado.

Subscrição por 802.21

O MIH User envia uma mensagem de subscrição de eventos especificando uma periodicidade para que lhe sejam enviadas mensagens a informação de contexto subscrita.
Opcionalmente, pode ser utilizada uma mensagem de configuração de limiares. Esta mensagem permite a configuração de valores para condições limite dos dados de contexto. Cada vez

que estes limites forem transpassados é enviada uma mensagem de notificação com o valor em causa.

As figuras 4.11 e 4.12 representam os diagramas de sequência implementados para a troca de mensagens efectuada pelo mecanismo de subscrição/configuração.

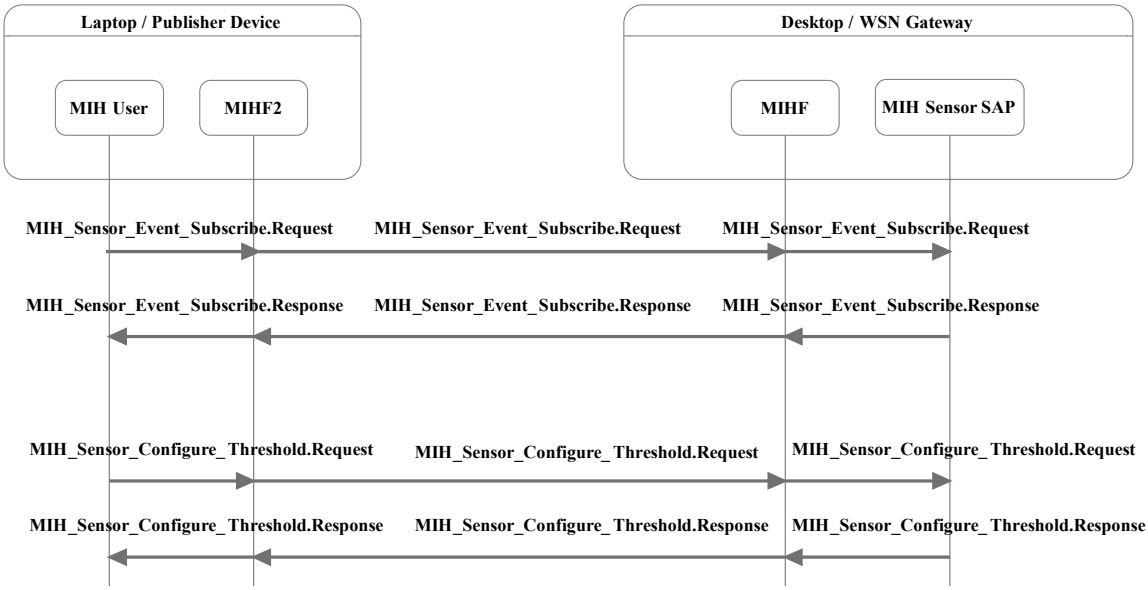


Figura 4.11: Mecanismo de Subscrição/Configuração accionado pelo MIH User do Utilizador Publicador

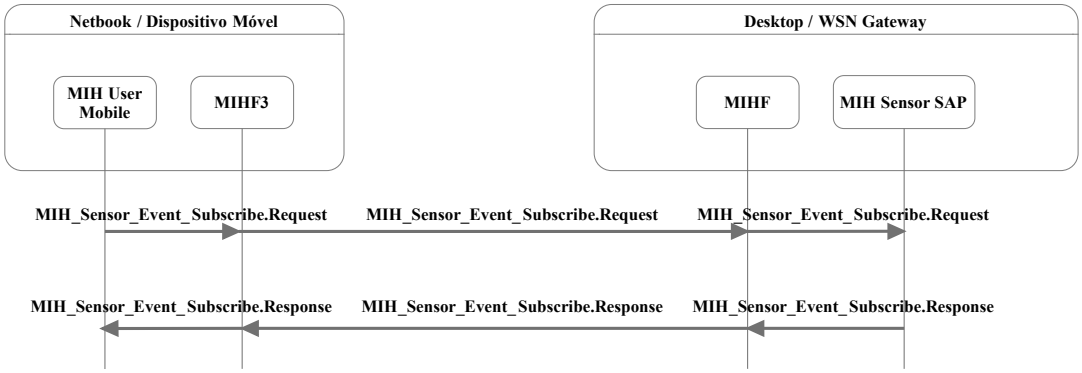


Figura 4.12: Mecanismo de Subscrição/Configuração accionado pelo MIH User do Utilizador Móvel

Na implementação definiu-se que o utilizador móvel não teria permissão para utilizar a configuração de limiares pois condicionava a escalabilidade da *gateway* de sensores, uma vez que se o número de utilizadores móveis aumentasse consideravelmente o processamento necessário para controlar as variáveis de decisão nos controlos de limite tornar-se-íam demasiado onerosos. Por este motivo, o utilizador Móvel utiliza apenas as mensagens de subscrição de

eventos, podendo indicar um período mais curto para a recepção de mensagens de informação de contexto. Com esta alternativa, o processamento da informação para controlo de valores e condições aceitáveis fica a cargo do nó móvel.

4.6.4 Disponibilização de Informação

Para que o utilizador móvel tenha acesso a informação é preciso que esta esteja disponível e para esse fim é preciso que exista alguma entidade a publica-la.

Quando o suporte é efectuado através de 802.21 a *gateway* fornece directamente a informação aos utilizadores. Por outro lado, se o suporte for feito por XMPP a informação tem de ser publicada no PT Context Broker para que o utilizador móvel lhe tenha acesso.

A disponibilização de informação é efectuada com recurso a um **Context Provider**, embutido no utilizador publicador, que agrega a informação de contexto recebida pelo protocolo MIH 802.21 e publica-a para o PT Context Broker.

Foi utilizado também o *webservice* Pachube como serviço de informação de contexto, a publicação para este *webservice* é feita por HTTP e utiliza-se esta plataforma como meio complementar de consulta de informação de contexto. As figuras 4.13, 4.14, 4.15 representam os diagramas de sequência utilizados na implementação do *Context Provider* e reflecte as trocas de mensagens realizadas entre este, o PT Context Broker e o Pachube.

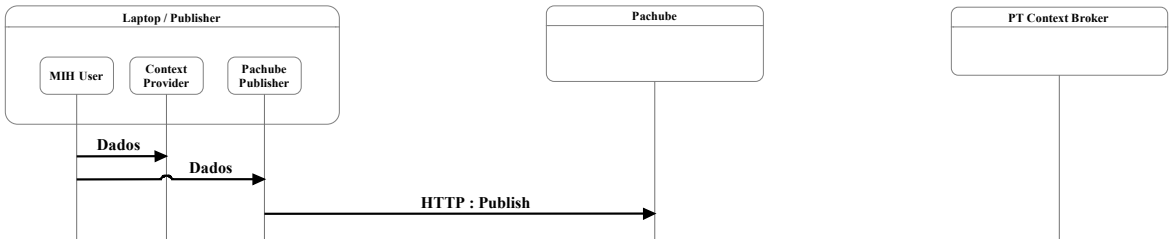


Figura 4.13: Mecanismo de disponibilização de informação para o Pachube

A figura 4.13 demonstra a sequência de mensagens através da qual a informação é publicada no *website* Pachube. Neste caso, o Pachube Publisher limita-se a enviar a informação por HTTP para o *webservice*.

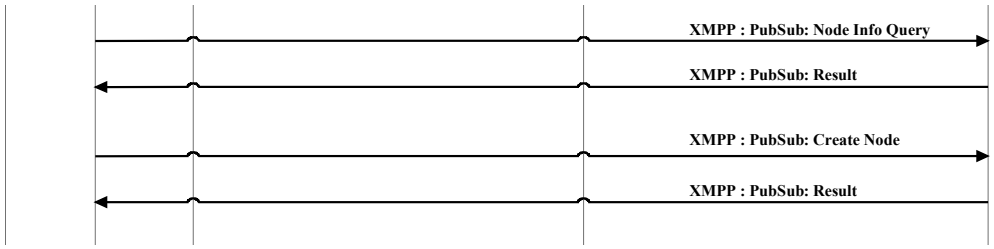


Figura 4.14: Mecanismo de verificação de nós no PT Context Broker

A figura 4.14 demonstra a sequência de mensagens através das quais é efectuada a verificação do estado do nó para o qual se deseja publicar. O *Context Provider* necessita de verificar algumas condições antes de proceder à publicação propriamente dita. Primeiramente verifica a existência e disponibilidade do nó para qual irá publicar. Se este existir procede directamente à publicação, caso contrario cria o nó e depois publica.

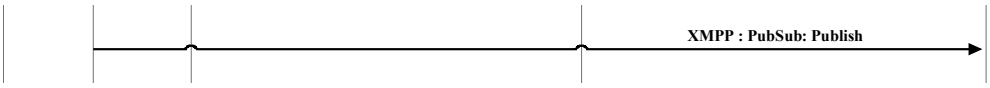


Figura 4.15: Mecanismo de disponibilização de informação para o PT Context Broker

A figura 4.15 demonstra a sequência de mensagens através das quais é publicada a informação. Os dados após serem recolhidos pelo MIH User do utilizador publicador através do protocolo MIH 802.21 são enviados para o *Context Provider* que, já tendo a certeza de que o nó existe e está acessível publica a informação.

Pode verificar-se, por análise das figuras apresentadas, que são enviadas mensagens PubSub por XMPP para verificar o estado do nó (*Node Info Query*) e através da resposta (Result) analisa a sua existência. Mediante essa mensagem, pode criar o nó enviando a mensagem *Create Node*. Finalmente e após estarem reunidas as condições para publicação, é enviada a mensagem *Publish* por XMPP contendo os dados e a informação de contexto a ser publicada.

4.6.5 Consumo de Informação

A informação de contexto fornecida pela rede de sensores pode ser consumida por duas formas distintas, pelo protocolo MIH 802.21 e pelo protocolo XMPP. Os cenários criados incidem sobre estas duas formas de consumo de informação e os mecanismos que despoletam cada uma.

A decisão da forma de acesso utilizada para o consumo de informação é tomada pelo MIH Sensor SAP em conjunto com a MIHF da *gateway* da rede de sensores e pode ser baseada em vários factores, no entanto esses factores não foram abordados nesta dissertação podendo apenas ser exemplificados/sugeridos pelo controlo de recursos de processamento da *gateway*, condições da ligação ou topologia da rede.

Consumo por 802.21

O consumo por 802.21 é realizada no cenário 4.5.1 onde a *gateway* providencia a ambos utilizadores recursos para obterem a informação de contexto via extensão para sensores do protocolo MIH 802.21.

Começando pelo **MIH User do utilizador publicador**, após a subscrição de eventos e a configuração de limiares, este utilizador fica habilitado a consumir informação de contexto através de três formas distintas, notificações periódicas, notificações geradas pelo transpassamento de limiares e através do mecanismo de Pergunta/Resposta.

A figura 4.16 ilustra o diagrama de sequência utilizado na implementação com a representação do consumo da informação de contexto através da recepção de mensagens de protocolo MIH 802.21.

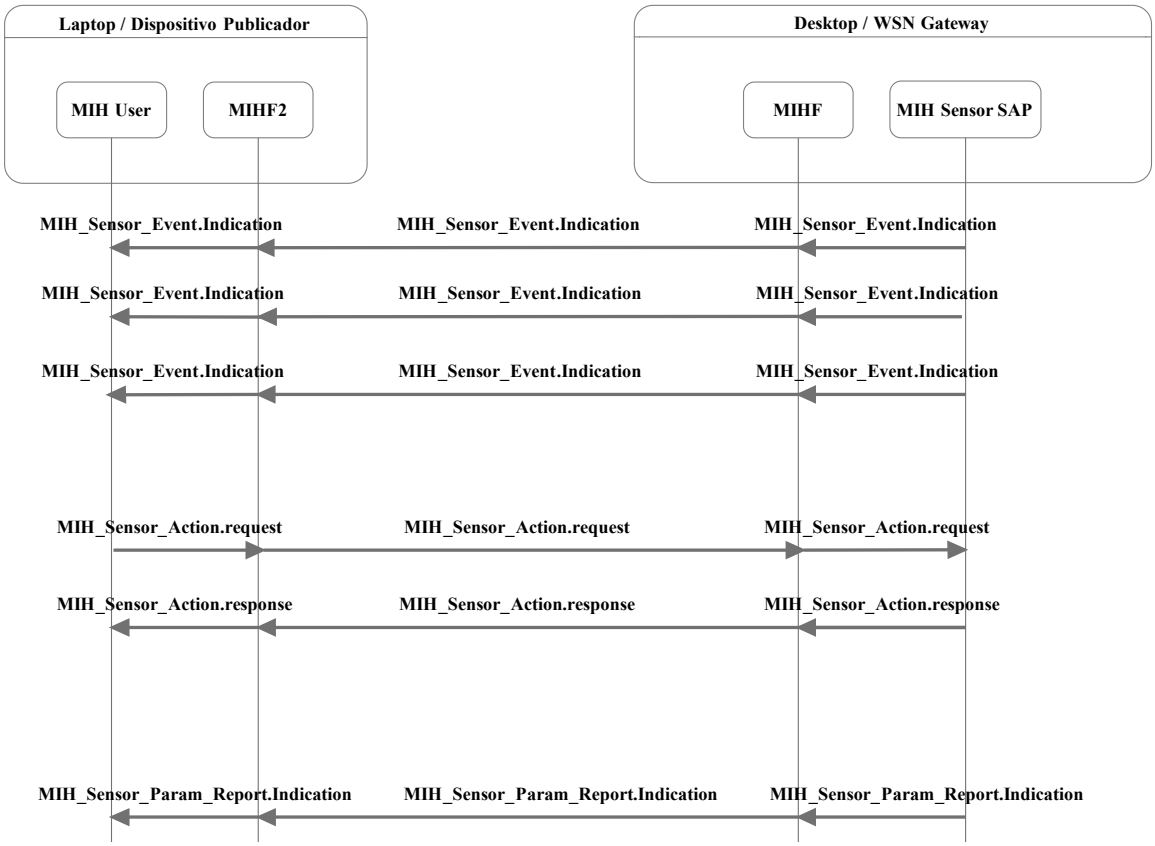


Figura 4.16: Mecanismo de Consumo de Informação pelo MIH User do utilizador publicador

Analisando os três formas de consumo ilustradas na figura, as primeiras três mensagens, do tipo MIH_Sensor_Event.Indication, são exemplos das mensagens resultantes da subscrição de eventos. Estas mensagens são geradas com uma periodicidade especificada aquando do processo de subscrição. Seguidamente, observa-se o mecanismo de Pergunta/Resposta com recurso às mensagens MIH_Sensor_Action. A ultima forma de consumo é representada pela mensagem MIH_Sensor_Param_Report.Indication. Esta mensagem é despoletada pelo transpassamento de um valor de limiar especificado aquando do processo de configuração de limiares.

O **MIH User do utilizador móvel** apresenta uma quantidade de consumo de informação ligeiramente inferior. Este facto deve-se às características inerentes aos nós móveis de uma rede, além da sua capacidade de processamento ser tipicamente inferior a um nó estacionário (como o utilizador publicador), o número de nós móveis também é expectavelmente superior causando sobrecarga de processamento na gateway.

Esta entidade só possui duas formas de consumo de informação, através de notificações periódicas criadas pela subscrição de eventos e através do mecanismo Pergunta/Resposta. Assume-se que o processamento da informação recolhida é da responsabilidade do utilizador e como forma de poder tomar decisões mais exactas uma vez que não dispõe do mecanismo de configuração de limiares, a periodicidade das mensagens geradas pelos eventos que subscreve é substancialmente inferior. Com esta assumpção consegue-se um compromisso entre a falta de um mecanismo de obtenção de informação e a necessidade de efectuar operações tendo em conta em factores de decisão baseados na informação de contexto.

A figura 4.17 ilustra o diagrama de sequência utilizado na implementação com a representação do consumo da informação de contexto através da recepção de mensagens de protocolo MIH 802.21.

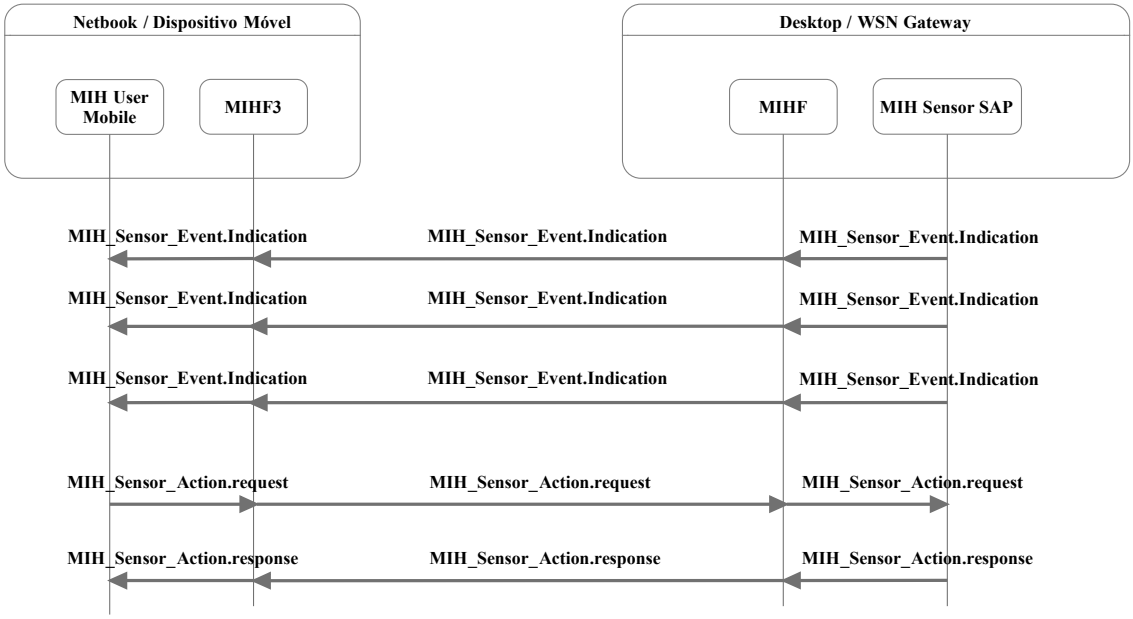


Figura 4.17: Mecanismo de Consumo de Informação pelo MIH User do utilizador móvel

Analogamente ao consumo de informação pode analisar-se a figura verificando que existem três mensagens do tipo MIH_Sensor_Event.Indication, que são exemplos das notificações resultantes da subscrição de eventos. Além deste mecanismo, pode verificar-se que pode ser utilizado, o mecanismo de Pergunta/Resposta com recurso às mensagens do tipo MIH Sensor Action.

Consumo por XMPP

O consumo de informação através do protocolo XMPP é executado no segundo cenário 4.5.2. Neste cenário, a *gateway* não disponibiliza recursos para suporte directo de informação de contexto através do protocolo MIH 802.21 ao utilizador móvel e delega essa função para o PT Context Broker através do protocolo XMPP.
Nesta situação o MIH User do utilizador publicador mantém-se com o seu acesso à informação de contexto por 802.21 uma vez que se assume que este utilizador é privilegiado em termos de

recursos para acesso directo. No entanto, o MIH User do utilizador móvel, após o mecanismo de descoberta de capacidades é informado de que se desejar obter informação de contexto necessita de subscrever um nó num servidor XMPP (PT Context Broker) cujo endereço lhe é indicado na mesma mensagem.

A figura 4.18 ilustra o diagrama de sequência utilizado na implementação com a representação do consumo da informação de contexto através da recepção de mensagens de protocolo XMPP.

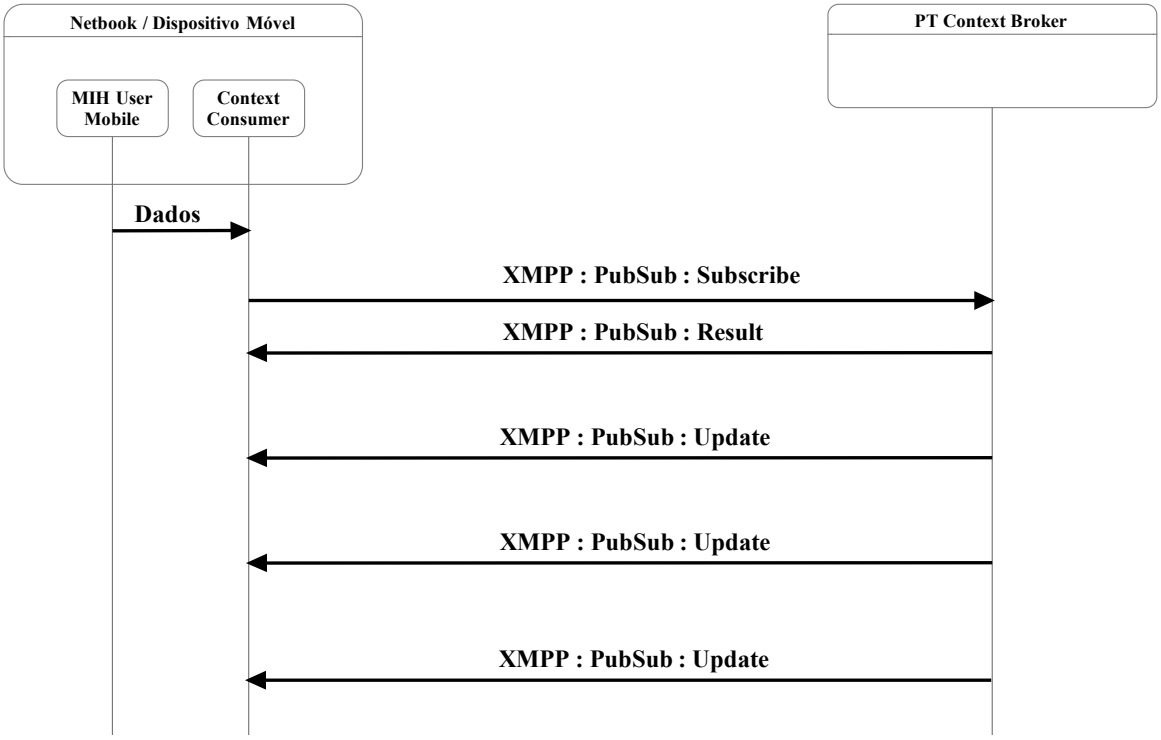


Figura 4.18: Mecanismo de Consumo de Informação pelo MIH User do utilizador móvel

Assim que o **MIH User do utilizador móvel** recebe o endereço do servidor XMPP e nó de publicação através do processo de descoberta de capacidades contacta o servidor XMPP (PT Context Broker) subscrevendo o nó indicado. Concluída com sucesso o processo de subscrição, o utilizador recebe uma mensagem PubSub de XMPP com os últimos dados actualizados que esse nó contém. Ao longo do tempo o PT Context Broker irá enviar mensagens Update com a informação de contexto subscrita, cada vez que a informação no nó for actualizada.

4.7 Comunicação 802.21

No conceito de solução apresentado no cenário de teste podem-se identificar três entidades centrais que utilizam este protocolo e é a relação entre estes elementos que coloca em movimento todo o cenário testado, o desktop, o laptop e o netbook. Do ponto de vista do protocolo 802.21, estas três entidades e as suas relações podem ser ilustradas pela figura 4.19.

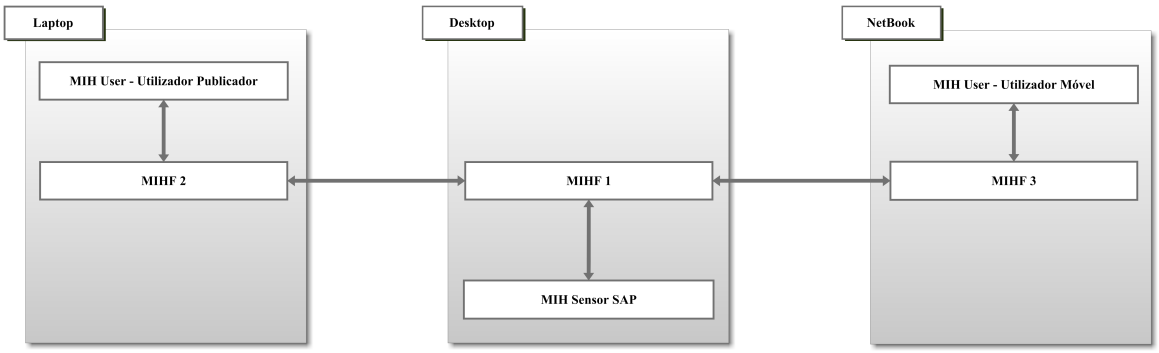


Figura 4.19: Ponto de vista do 802.21

Pode-se, à partida, apenas pela análise da figura 4.19 identificar quatro componentes distintos, os MIH Users(MIH User do Utilizador Publicador e o MIH User do Utilizador Móvel), as MIHFs, a MIH Sensor SAP e interligando estes elementos, o protocolo MIH.

Na implementação e desenvolvimento desta versão do protocolo MIH foi utilizada uma abordagem em conformidade com o príncipio *Open-Closed*. Embora o protocolo tenha sido estendido, o seu formato, regras e moldes gerais não foram modificados.

4.7.1 MIH Sensor SAP

Para possibilitar a comunicação entre o protocolo MIH 802.21 e a rede de sensores foi necessário desenvolver e implementar um SAP específico para a tecnologia em causa tendo sido denominado de MIH Sensor SAP.

No desenvolvimento deste componente MIH 802.21 foram tidas em conta duas *guidelines* fundamentais, abordagem generalista às novas capacidades, mensagens e mecanismos implementados para que possan ser aplicadas a qualquer tipo de redes sem fio de sensores mantendo o suporte a equipamentos diferentes e a adaptação das novas funcionalidades e mecanismos às regras e padrões de funcionamento já existentes nesta norma.

A implementação deste MIH Sensor SAP foi desenvolvida de acordo com a figura 4.20 e define três blocos funcionais, Recolha de dados, Armazenamento Local e Comunicação 802.21.

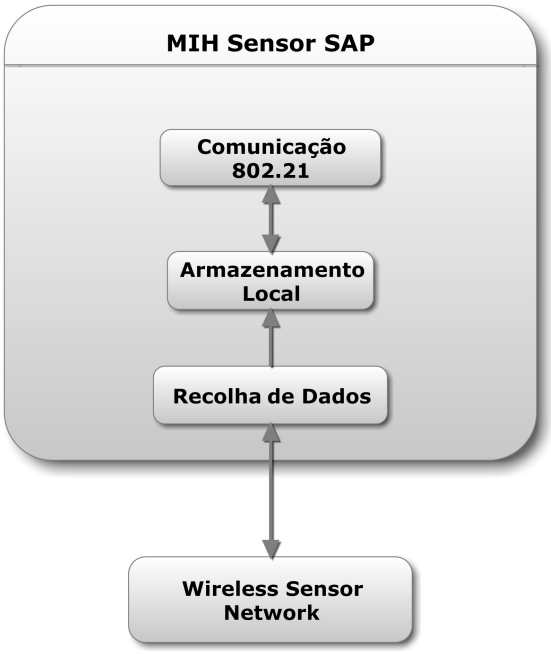


Figura 4.20: MIH Sensor SAP

A informação recolhida da rede de sensores é testada quanto a sua validade no módulo de **Recolha de Dados** que ao mesmo tempo se encarrega de a depositar num módulo repositório de informação, **Armazenamento Local**. O MIH Sensor SAP encapsula também um módulo de comunicação MIH 802.21. Este módulo diz respeito a todo o processo de gestão e disponibilização de informação de sensores para a rede através de 802.21.

Recolha de Dados

Como já referido, o módulo de **Recolha de Dados** coloca-se à escuta num porto de comunicação designado e recebe a informação da *basestation* dos sensores depositando-a no módulo de Armazenamento Local. Previamente à recepção dos dados no módulo da Recolha de Dados estes são filtrados pela *basestation* para detectar anomalias nos valores.

Armazenamento Local

Este módulo serve de repositório para os dados recolhidos através dos sensores. É composto por um processo que se coloca à escuta num porto local designado e recebe informação pelo módulo de Recolha de Dados pelo que se assume que os valores que se encontram neste módulo são sempre válidos no contexto em que se encontram. O Armazenamento Local disponibiliza sempre os valores actualizados pelo que cada leitura a este módulo retornará, os valores mais recentes até esse instante.

Módulo de Comunicação 802.21

O módulo de comunicação 802.21 tem como função gerir as mensagens MIH relativas a informação de sensores interagindo com o Armazenamento Local para aceder à informação actual dos sensores. A figura 4.21 representa o modelo de funcionamento interno deste módulo através de um diagrama de actividades.

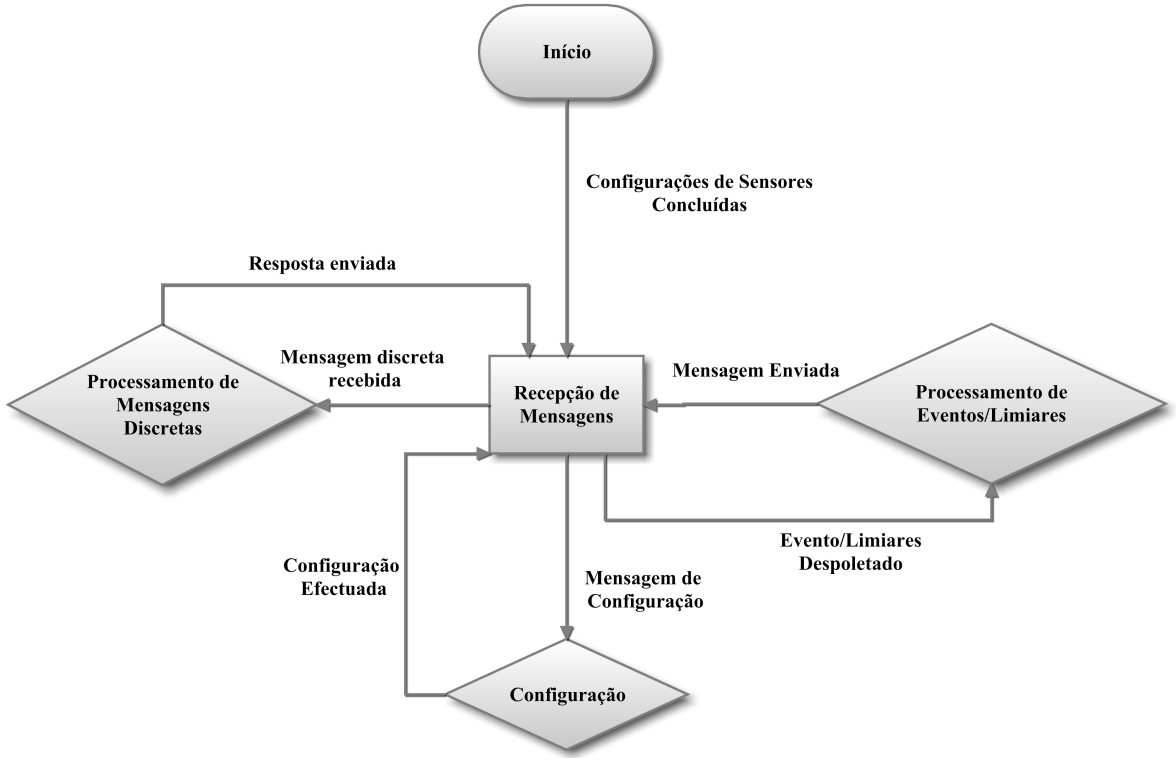


Figura 4.21: Diagrama de Actividades da Comunicação 802.21

Este processo inicia-se com a configuração dos sensores, é enviado para os sensores o código necessário para o seu funcionamento mediante os parâmetros estabelecidos, assim que essa informação está concluída os sensores estão prontos para iniciar a sua recolha de dados e a comunicação 802.21 pode ser iniciada. De seguida o módulo entra no estado de **Recepção de Mensagens**, neste estado o módulo limita-se a esperar por mensagens locais ou remotas. Este estado engloba ainda uma monitorização dos valores dos sensores.

A partir da Recepção de Mensagens podem derivar três acções diferentes, o Processamento de Eventos/Limiares, a Configuração e o Processamento de Mensagens Discretas.

Quando é enviada uma mensagem de subscrição ou de configuração de limiares é despoletada a acção **Configuração** que procede às configurações solicitadas, envia uma mensagem de resposta informando o sucesso ou insucesso do processo de configuração e retorna ao estado de Recepção de Mensagens.

Cada vez que, durante a monitorização dos valores dos sensores no estado de Recepção

de Mensagens, existe um limiar ou um período de subscrição atingidos é accionado o **Processamento de Eventos/Limiares** que recolhe os dados que dizem respeito à notificação despoletada, envia a mensagem correspondente ao MIH User respectivo e retorna ao estado de Recepção de Mensagens.

O **Processamento de Mensagens Discretas** processa-se quando é recebida uma mensagem correspondente ao mecanismo Pergunta/Resposta como por exemplo uma mensagem MIH Sensor Action. Este tipo de mensagens é independente do funcionamento de todos os mecanismos automáticos e não depende de valores temporais ou sensoriais e é utilizado apenas pelos MIH Users. Aquando da recepção de uma mensagem deste tipo, é feito o *parsing* e identificado o tipo de acção requerido, após a execução da acção em questão é enviada uma mensagem que informa o sucesso ou insucesso dessa acção e opcionalmente podem ser encapsulados parâmetros requisitados como valores de sensores ou estado dos dispositivos.

4.7.2 MIH User - Publicador

O MIH User - Publicador é a entidade 802.21 que garante a publicação da informação de contexto nos servidores que lhe são indicados. Este componente subscreve e configura limiares remotamente com o MIH Sensor SAP do qual deseja obter informação ao mesmo tempo que dispõe do mecanismo Pergunta/Resposta MIH Sensor Action para obter dados instantaneamente.

A arquitectura implementada para prova de conceito assume que este componente possui comunicação constante por 802.21 com o MIH Sensor SAP para que a informação de contexto esteja sempre disponível através do protocolo MIH.

A implementação deste componente baseou-se no modelo da figura 4.22. Internamente o MIH User Publicador é composto por dois módulos de funcionamento, a Comunicação 802.21 e a Recolha e Envio de Dados. Externamente, funciona emparelhado com outros dois componentes responsáveis pela publicação e disponibilização da informação de contexto por meios de comunicação alternativos ao 802.21.

Figura 4.22: Modelo de Componentes do MIH User Publicador

A **Comunicação 802.21** é o módulo responsável pela gestão da comunicação entre o MIH User Publicador e o MIH Sensor SAP. É da responsabilidade deste processo garantir que a comunicação é mantida e a informação de contexto é obtida correctamente e de acordo com as necessidades explicitadas para publicação.

O módulo de **Recolha e Envio de Dados** representado na figura recebe a informação e os dados recolhidos através de *parsing* das mensagens MIH 802.21 e reencaminham-nos por sockets para os dois processos externos, Context Provider e Pachube Publisher. O funcionamento deste módulo apenas depende das mensagens recebidas pelo módulo de Comunicação 802.21.

A figura 4.23 representa o modelo de diagrama de actividades seguido no funcionamento do módulo de Comunicação 802.21 do MIH User Publicador.

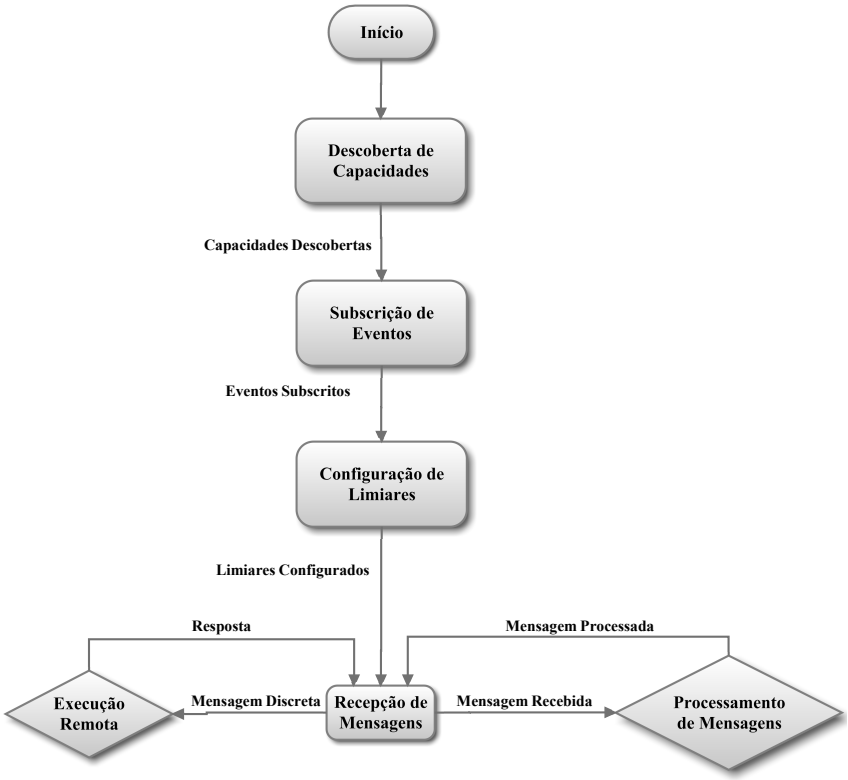


Figura 4.23: Modelo de Diagrama de Actividades do MIH User Publicador

O diagrama representa um processo com quatro estados principais, a Descoberta de Capacidades, a Subscrição de Eventos, a Configuração de Eventos e a Recepção de Mensagens. Complementar a estes estados existem duas acções disponíveis, a Execução Remota e o Processamento de Mensagens.

No estado de **Descoberta de Capacidades** é enviado por *broadcast* uma mensagem MIH Sensor Capability Discover com o intuito de receber, da MIH Sensor SAP disponível a informação sobre as capacidades MIH para sensores que suporta.

Após a descoberta de capacidades o processo entra no estado de **Subscrição de Eventos**. Neste estado é enviada uma mensagem MIH Sensor Event Subscribe para a MIH Sensor SAP informando os eventos que deseja subscrever e com que periodicidade. Em resposta o MIH Sensor SAP informa sobre o sucesso ou insucesso da subscrição.

O estado de **Configuração de Limiares** ocorre após a subscrição de eventos e tem como objectivo configurar um conjunto de valores limite para os quais a MIH Sensor SAP deverá emitir uma notificação cada vez que forem transpassados. Este procedimento efectua-se através de um comando MIH Sensor Configure Threshold.

Estando concluidos os estados de descoberta, subscriçao e configuração o processo entra no seu estado de funcionamento contínuo, a **Recepção de Mensagens**. Este estado permite ao MIH User Publicador receber as notificações de eventos e de transpassamento de limiares que serão gerados ao longo do tempo e enviar mensagens com pedidos de execução remota. Quando uma mensagem é recebida, é despoletada a acção de **Processamento de Mensagem** que interpreta a mensagem e actua conforme definido à priori no âmbito da publicação. Eventualmente, o MIH User Publicador pode emitir mensagens MIH Sensor Action para receber informação instantaneamente.

4.7.3 MIH User - Utilizador Móvel

O MIH User como utilizador móvel representa uma entidade que aborda uma rede com o intuito de receber informação de contexto e encontra, à partida, dois mecanismos para o conseguir, através do protocolo MIH 802.21 e através do acesso a um servidor externo (*Context Broker*).
A figura 4.24 ilustra o modelo funcional da implementação utilizada para desenvolver esta entidade.

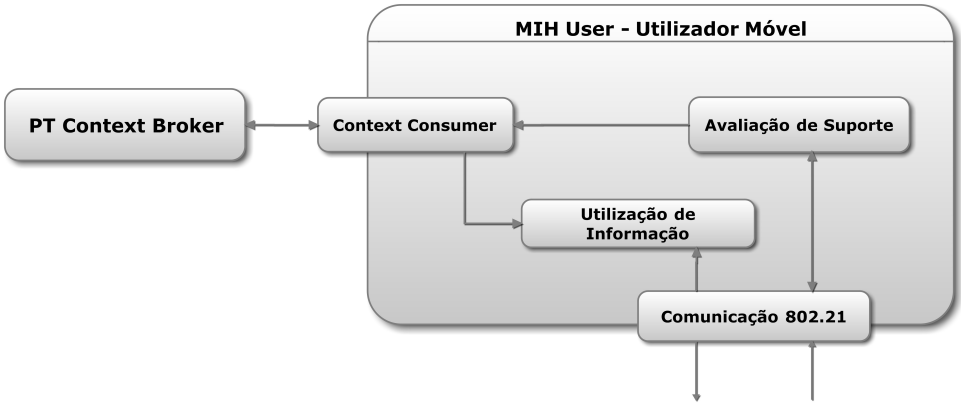


Figura 4.24: Modelo de Funcionamento do MIH User do utilizador móvel

Utilizam-se quatro módulos funcionais para a construção desta entidade, a Comunicação 802.21, o Context Consumer, a Avaliação de Suporte e a Utilização de Informação.

Durante o processo de descoberta de capacidades realizado pelo módulo de **Comunicação 802.21**, é informado ao utilizador se a rede suporta transporte de informação de contexto contínua através do protocolo MIH 802.21 ou, em caso dos recursos necessários para esse suporte não estarem disponíveis, encapsula na sua resposta um endereço de um *Context Broker* onde essa informação está a ser publicada e os respectivos nós de publicação. Esta mensagem de descoberta de capacidades é analisada pelo módulo de **Análise de Suporte** que após o *parsing* da mensagem avalia o suporte indicado e toma as medidas necessárias para continuar com o acesso à informação através de 802.21 ou desligar este módulo e activar o módulo de Comunicação XMPP. Nas situações em que é disponibilizado o endereço do *Context Broker* e o módulo **Context Consumer** é activado, este entra em contacto com o *Context Broker* subscrevendo os nós de publicação que lhe foram indicados pelo processo de descoberta de capacidades. Assim que a informação de contexto chega efectivamente ao MIH User, seja por XMPP ou 802.21, esta é depositada no módulo de **Utilização de Informação** que agrega a informação recebida e a dispõe para análise ou visualização.

O funcionamento do módulo de **Comunicação 802.21** implementa o diagrama de actividades ilustrado na figura 4.25.

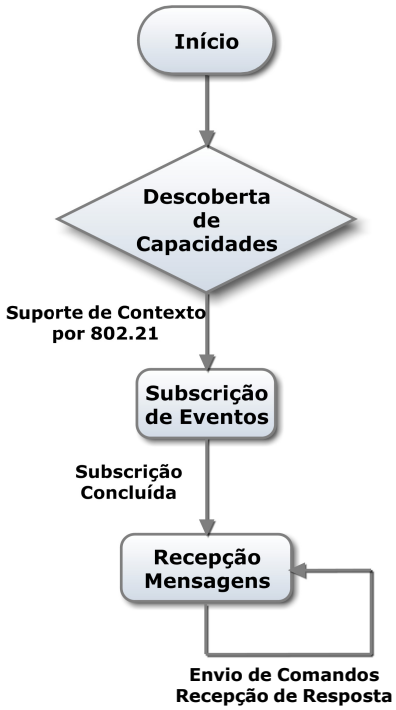


Figura 4.25: Diagrama de actividades do MIH User do utilizador móvel

Inicialmente, é efectuado o mecanismo de **Descoberta de Capacidades** enviando uma mensagem MIH Sensor Capability Discover por *Broadcast*. Como resposta a esta mensagem a MIH Sensor SAP informa das capacidades de que dispõe bem como do tipo de suporte de acesso à informação de contexto. Sobre esta mensagem é avaliada a resposta quanto ao

suporte de acesso. Quando o transporte pelo protocolo 802.21 é suportado, o mecanismo de **Subscrição de Eventos** encarrega-se de enviar uma mensagem MIH Sensor Event Subscribe subscrevendo os eventos necessários com a periodicidade desejada.
Após uma subscrição bem sucedida o processo entra no estado de **Recepção de Mensagens**. Neste estado serão aguardadas e recebidas as mensagens de MIH Sensor Event respeitantes aos eventos subscritos com uma periodicidade previamente especificada.
Opcionalmente, o utilizador dispõe do já referido mecanismo de Pergunta/Resposta instantânea através das mensagens de MIH Sensor Action.

4.7.4 MIH Functions

Na prova de conceito utilizada, tal como demonstrado foram utilizados três equipamentos para teste, o laptop, o dektop e o netbook. Cada equipamento possui uma MIHF local para possibilitar a comunicação entre os mesmos.

A figura 4.26 representa a comunicação e as várias MIH Functions colocadas nos equipamentos para prova de conceito.

Figura 4.26: Modelo de Funcionamento das MIH Functions

Na implementação desenvolvida, as MIHFs desempenham um papel fundamental na comunicação entre as várias entidades uma vez que se encarregam do reencaminhamento das mensagens entre as unidades de mais baixo nível (MIH Sensor SAPs) e as unidades de mais alto nível (MIH Users).

As MIHFs utilizadas são baseadas na implementação desenvolvida para o projecto ODTONE e podem ser consideradas como genéricas do ponto de vista do *standard* 802.21 pelo que para suportarem o transporte de contexto foram implementadas extensões descritas na secção 4.10.

4.8 Comunicação Alternativa

A comunicação alternativa sugerida aponta para a utilização de um Context Broker como suporte alternativo para o acesso a informação de contexto quando os meios usuais não se encontram disponíveis.

O *Context Broker* apenas pode criar a camada de inteligência esperada se lhe for disponibilizada informação para tal. Na prova de conceito apresentada foi utilizado um *Context Provider* associado ao MIH User do Utilizador Publicador para publicar informação para o *Context Broker* e um *Context Consumer* associado ao MIH User do Utilizador Móvel para consumir a informação publicada.

Redundância

Na prova de conceito apresentada, a redundância no acesso à informação é criada através do protocolo XMPP. O facto do protocolo XMPP poder ser utilizado com base numa arquitectura Publicador/Subscritor torna-se bastante positivo, à semelhança do que ocorre com as mensagens de subscrição de eventos no protocolo MIH 802.21, o mecanismo PubSub permite o envio imediato de mensagens a cada actualização de informação. Ao nível da rapidez e facilidade na distribuição de informação, o acesso à informação por esta alternativa não fica muito atrás da comunicação por 802.21.

4.8.1 Context Broker

Foi utilizado o PT Context Broker (ver Anexo C) como *Context Broker*, composto por um servidor XMPP com mecanismo PubSub.

Organização de Informação

Os nós de PubSub do PT Context Broker estão estruturados numa organização hierárquica do mais genérico para o mais específico. A denominação utilizada segue uma regra onde o nó Collection está a cima e agrega nós Leaf. O tipo de nó Leaf é justaposto ao nome do Collection a que está associado ficando com um formato "Collection:Leaf".

A figura 4.27 representa a estrutura conceptual da organização interna de informação no PT Context Broker.

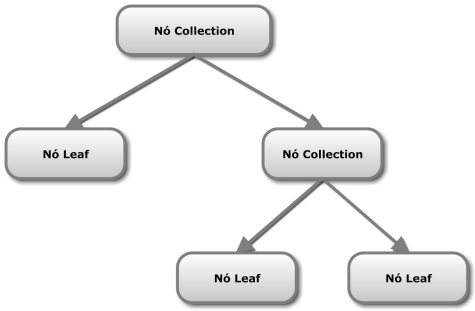


Figura 4.27: Estrutura da organização da informação.

A figura 4.28 ilustra um exemplo da organização de possíveis nós criados pela prova de conceito no PT Context Broker.

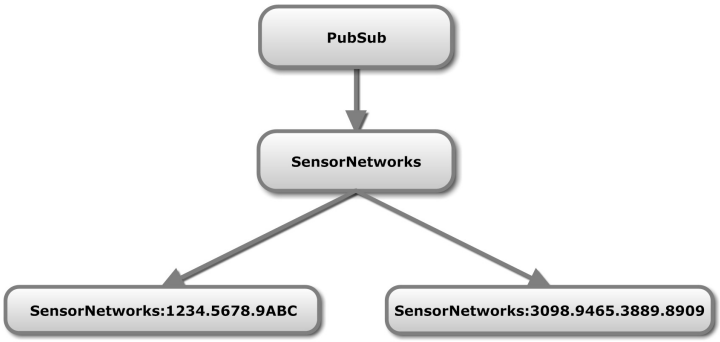


Figura 4.28: Estrutura da organização da informação.

Na implementação definiu-se que o nó Collection denominar-se-ía SensorNetworks e as Leafs criadas seriam o endereço MAC da *basestation* à qual estão conectados os Sun Spots. Esta informação é explicitada pela MIH Sensor SAP nas mensagens de MIH Sensor Capability Discover.

4.8.2 Context Provider

O Context Provider é uma entidade que recebe informação via inter-processo do MIH User do Utilizador Publicador e, através de um modelo baseado no protocolo XMPP, publica a informação para um nó que se encontra no *Context Broker*.

A figura 4.29 representa o modelo de funcionamento do *Context Provider* implementado.

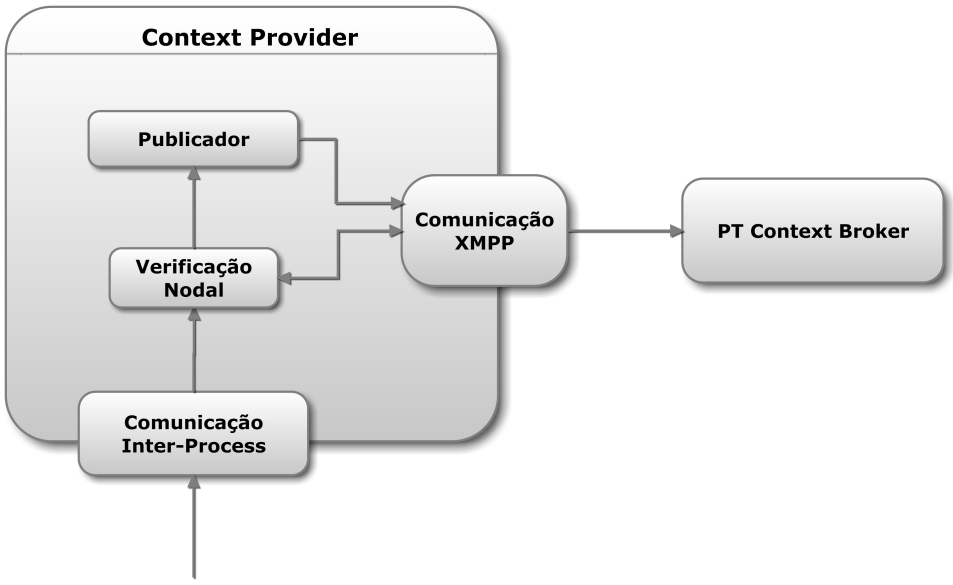


Figura 4.29: Modelo de Funcionamento do Context Provider

Como se pode analisar pela figura 4.29, o Context Provider implementado é composto por quatro módulos, Comunicação *Inter-Process*, Verificação Nodal, Publicador e Comunicação XMPP. O MIH User do Utilizador Publicador envia uma mensagem por socket com informação de contexto e a informação sobre o *Context Broker* necessária para publicação. Esta informação é recebida pelo módulo **Comunicação Inter-Process** que separa a informação de contexto dos dados de referência para publicação. Após este passo o módulo **Verificação Nodal** vai verificar a existência dos nós para os quais irá publicar.
Depois da Verificação Nodal estar concluída é informado ao **Publicador** sobre a existência dos nós em questão. Se os nós não existirem, antes de publicar a informação, o Publicador encarrega-se de os criar. Só após a confirmação da existência destes nós pode a informação ser publicada.
Tanto o módulo de Verificação Nodal como o Publicador utilizam o módulo **Comunicação XMPP** para, utilizando o mecanismo PubSub, do protocolo XMPP, obter informação e gerir os nós associados.

A figura 4.30 representa o diagrama de actividades seguido na implementação do Context Provider.

Figura 4.30: Diagrama de Actividades do Context Provider

Quando é recebida uma mensagem, a sua decomposição dá origem à obtenção dos nós para publicação, do endereço do servidor e da informação de contexto a ser publicada, este mecanismo é representado na figura pelo estado **Recepção de Mensagens**.

Após a decomposição da mensagem os nós serão verificados quanto à sua existência nos estados **Verificação de Nó Collection** e **Verificação de Nó Leaf**. Primariamente será analisado a existência do nó Collection, caso não exista, será criado e será efectuado o mesmo procedimento para o nó Leaf.

Garantida a existência de ambos nós, o processo entra no estado **Publicação** onde serão publicados os dados para os respectivos nós.

4.8.3 Context Consumer - Utilizador Móvel

O *Context Consumer* está associado ao MIH User do Utilizador Móvel ilustrado na figura 4.24. Este elemento tem como função obter a informação de contexto publicada no *Context Broker*.

A figura 4.31 representa o diagrama de actividades seguido na implementação do *Context Consumer*.

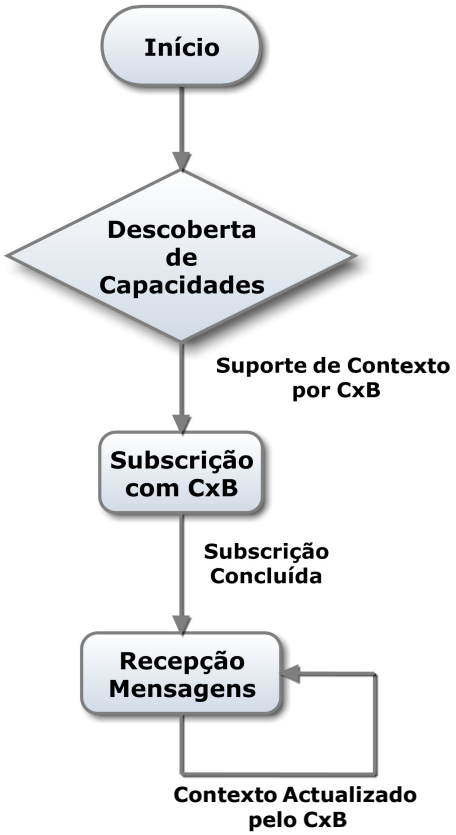


Figura 4.31: Diagrama de Actividades do Context Consumer

No mecanismo de descoberta efectuado pelo MIH User do Utilizador Móvel é incluido na mensagem de resposta o endereço do servidor e os nós a subscrever para obter a informação de contexto disponibilizada pela rede. Com o endereço e os nós que obtém, o *Context Consumer*

efectua uma subscrição utilizando o mecanismo PubSub. Após a subscrição receberá mensagens sobre a informação de contexto cada vez que o nó for actualizado no *Context Broker* pelo *Context Provider* associado ao MIH User do Utilizador Publicador.

4.8.4 Pachube Publisher

O Pachube *Publisher* é um componente que, à semelhança do *Context Provider*, está associado ao MIH User do Utilizador Publicador e ao receber a informação de contexto por *socket* publica-a no *webservice* Pachube (ver Anexo D).

A figura 4.32 representa o modelo de funcionamento do componente Pachube *Publisher*.

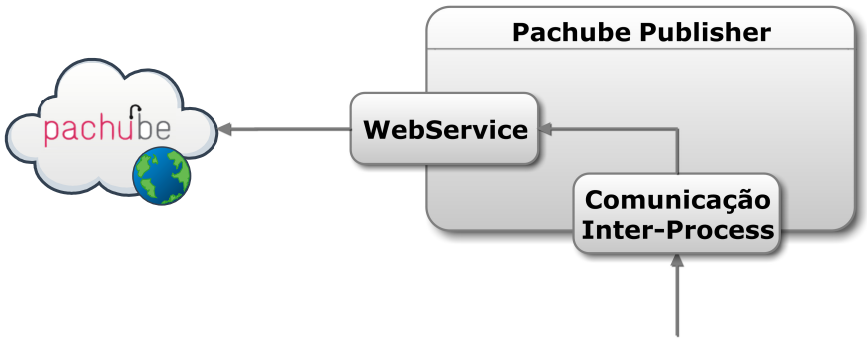


Figura 4.32: Modelo de Funcionamento do Pachube Publisher

O MIH User do Utilizador Publicador envia por *socket* para o processo do Pachube *Publisher* a mensagem com os dados a publicar e este encarrega-se de os formatar com as definições estipuladas pelo Web Service que as publica por HTTP. Assume-se à partida de que já existe um feed pré-configurado e que o módulo WebService já tem conhecimento do mesmo, assim sendo a criação ou manutenção do *feed* é-lhe transparente.

4.8.5 Consulta por Localização - Pachube

O Pachube é um serviço que agrega informação sensorial com o Google Maps. Por este motivo não se torna necessário informar o utilizador móvel do seu endereço ou do *feed* em questão uma vez que uma navegação ou uma procura no mapa rapidamente revelam as informações procuradas.

Na implementação desenvolvida o Pachube foi utilizado como ferramenta extra para visionar a correcta publicação de dados e ao mesmo tempo avaliar o potencial do *webservice* como Context Broker.

4.9 Organização da Rede de Sensores

A rede de sensores utilizada na prova de conceito foi composta por nós independentes que apenas comunicam com uma entidade que centraliza a informação. Cada nó é composto fisicamente por um dispositivo SunSpot e a entidade centralizadora de informação é uma

basestation da Sun Spot.
A figura 4.33 representa a organização física da rede de sensores utilizada como recurso a Sun Spots.

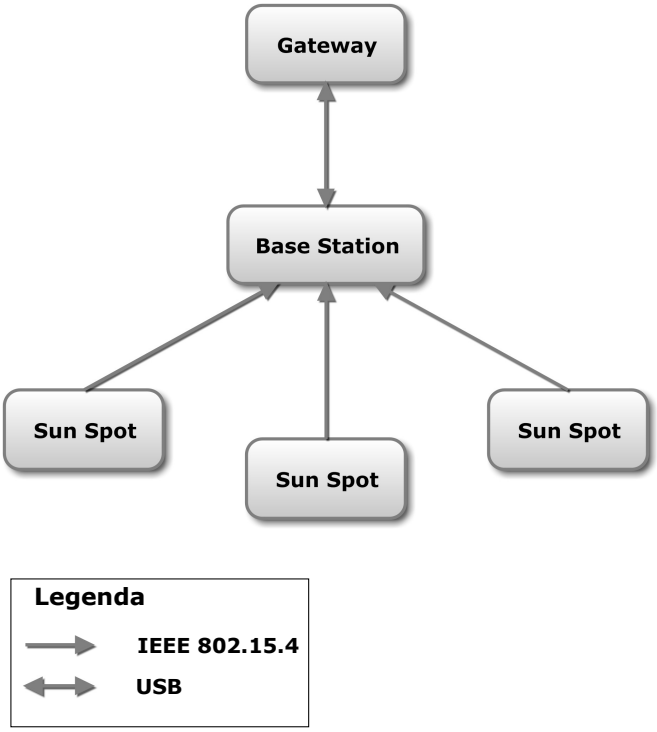


Figura 4.33: Organização da rede de sensores

Os Sun Spots fornecem informação de contexto baseada em temperatura, luminosidade e aceleração. Esta informação é enviada por 802.15.4 para a *basestation* designada que filtra dados por anomalias e os envia para a *gateway* associada. A *gateway* da implementação é composta pelo MIH Sensor SAP do desktop.

4.9.1 Configurações

Colocaram-se dois Sun Spots a recolher e enviar dados para a *basestation*. Os dados após filtragem na *basestation* são enviados para a *gateway* por *socket*. Para o funcionamento descrito foram necessárias algumas configurações que se tornam relevantes de explicitar.

Sun Spots

Embora a programação comportamental relativa a recolha de informação seja idêntica nos dois dispositivos SunSpot os períodos configurados para a recolha de amostras são diferentes. Num dispositivo SunSpot, a recolha de dados é efectuada a cada 1000 milisegundos. No dispositivo SunSpot restante, a recolha de dados é efectuada a cada 3000 milisegundos. Esta diferenciação foi implementada como forma de verificação da capacidade de resposta e processamento da basestation num cenário onde os dispositivos possuem ritmos de funcionamento diferentes.

Basestation

A basestation além de receber os dados enviados pelos Sun Spots efectua uma filtragem dos mesmos antes de proceder ao envio para a *gateway*. Este passo intermédio deve-se ao facto de serem expectáveis anomalias ao nível da rede de sensores.

As anomalias podem surgir nas mais variadas formas, desde um sensor que se desliga, a avarias internas que provocam o envio de dados erróneos, a alterações de condições por mão humana (e.g. colocar um objecto por cima de um sensor de luz). Para que a informação de contexto possa ser disseminada de uma forma correcta é necessário garantir que estes valores díspares não são tidos em conta.

A verificação dos valores medidos pelos sensores é feita mediante uma implementação básica do algoritmo de sliding window, à excepção das medidas do sensor de aceleração. A cada 25 leituras é feita uma média dos valores obtidos. Com este algoritmo consegue-se eliminar alguns valores mais díspares.

4.10 Detalhes de Implementação

Os detalhes de implementação revelam alguns problemas encontrados ao longo da implementação da prova de conceito bem como a solução para os mesmos. É revelada também uma introspecção nas decisões tomadas perante algumas adversidades na definição da arquitectura.

4.10.1 Validação de Medidas de Sensores

A validação das medidas dos sensores é conseguida através de uma comparação entre os valores obtidos a cada instante com a média previamente calculada.

No arranque do sistema da rede de sensores é assumido um período inicial de 60 segundos em que as medidas obtidas podem oscilar devido ao tempo de convergência que os sensores por vezes apresentam até atingirem uma gama de valores minimamente estável. Durante este período não é feita a média de valores uma vez que os valores medidos servem apenas para despiste técnico.

A partir dos 60 segundos iniciais, os valores obtidos começam a ser comparados com uma média aritmética. Define-se também uma percentagem sobre a média para o desvio padrão. Por cada medida obtida é calculada a diferença entre a média obtida previamente e o valor actual, se o resultado for superior ao valor do desvio padrão o valor é descartado. Se o resultado for inferior ao desvio padrão então a média é recalculada tendo em conta esse valor. Devido à natureza díspar dos três tipos de sensores considerados, o desvio padrão é diferente para os três casos. Foram observadas medidas individuais recolhidas em contextos diferentes para se determinar o desvio padrão como factor de decisão aceitável para a prova de conceito em cada um dos sensores.

Sensor de Temperatura

O sensor de Temperatura possui uma particularidade que pode ser considerada problema de construção dos Sun Spots e influência a recolha de medidas por parte do sensor de tempe-

ratura. O facto do sensor de temperatura estar muito próximo do processador coloca o valor de temperatura medido em questão.
Não obstante deste pormenor de construção, devido à pequena oscilação dos valores de temperatura entre os diferentes Sun Spots (aproximadamente 3%) considerou-se um desvio de padrão de 10% como um valor aceitável.

Sensor de Luminosidade

O sensor de luminosidade, ao contrário do sensor de temperatura apresenta uma oscilação de medidas um pouco maior. Como os valores obtidos variam, normalmente na ordem dos 10%, decidiu-se colocar o desvio padrão com um valor de 15%.

Sensor de Aceleração

O sensor de aceleração é um sensor que fornece informação com uma natureza um pouco diferente das restantes. Deste tipo de sensor pode inferir-se quanto à existência de movimento e qual a aceleração e uma vez que os cenários de teste são ambientes estáticos, faz sentido que toda e qualquer alteração seja reportada. Por este motivo, a média aritmética dos valores medidos não reportaria uma representação lógica deste contexto. Perante os argumentos apresentados, o desvio padrão considerado foi 100%.

4.10.2 Interoperabilidade

Como a interoperabilidade também é um objectivo do projecto ODTONE, e a versão existente aquando do início desta dissertação recorria apenas à linguagem de programação C++, todos as as entidades e protocolo MIH da norma 802.21 utilizadas nesta dissertação foram implementadas de raíz na linguagem Java, contribuindo para o desenvolvimento de mais uma meta deste projecto, a API Java.

4.10.3 Tipos de Dados Java

No desenvolvimento da API do protocolo MIH 802.21 foi encontrado apenas um problema de base, a ausência específica de tipos de dados sem sinal, à excepção do *Char* que representa dois bytes sem sinal, na linguagem Java utilizada.

A implementação de um protocolo de redes cuja construção envolve maioritariamente a manipulação bit-a-bit e onde a sua especificação é efectuada com base em octetos e não bytes, tornou-se imperativo implementar estes tipos de dados. A sua definição e desenvolvimento compõe os alicerces de toda a implementação Java do protocolo MIH 802.2.

Solução Encontrada

Os tipos de dados necessários e exigidos pelo protocolo são:

UNSIGNED_INT(tamanho) - representa um inteiro sem sinal com o tamanho a especificar o número de octetos.

OCTET(tamanho) - array de octetos com o tamanho a especificar o comprimento do *array*. Cada octeto tem um valor de 0x00 a 0xFF codificados em network byte order.

4.10.4 Considerações sobre a MIHF Utilizada

As MIHFs utilizadas foram cedidas pelo ODTONE e não suportavam de origem a expansão do protocolo MIH 802.21. Assim sendo, e como o protocolo especifica que quando a MIH Function não reconhece o MID de uma mensagem deve descarta-la foi necessário instruir a MIH Function de que mensagens sobre as quais o MID não fosse conhecido deveria reencaminha-las simplesmente para o destinatário da mensagem.
A versão da MIHF incluída nesta implementação ainda não possui mecanismos dinâmicos de registo de Users ou SAPs. No início de cada cenário torna-se necessário a especificação através de um ficheiro de configuração dos endereços e denominação de cada MIH User e MIH Sensor SAP.

4.10.5 Implementação do Context Provider

No desenvolvimento do Context Provider foi inicialmente criado um modelo de XMPP *Component*. Para a implementação deste *component* foi utilizada a biblioteca Whack [22]. Durante os testes desta biblioteca foi descoberto um *bug* no *handler* das funções de descoberta de serviços e informação de nós pelo que a abordagem teve de ser alterada.

Como solução ao problema encontrado dividiu-se o *Context Provider* em dois sub-módulos, um XMPP *Client* e um XMPP *component*. Para que o *component* possa publicar para um nó é necessário que este exista, e como esta verificação não era possível com a biblioteca anterior e não existia mais nenhuma biblioteca de *components* disponível para Java a informação passa primeiro por um XMPP Client, implementado com recurso às bibliotecas Tinder [23] e Smack [24], que verifica a existência dos nós em questão. Após esta verificação, envia ao XMPP Component os dados para publicação encapsulados com um parâmetro composto por dois caracteres no formato "XZ". O caracter X refere-se ao estado do nó collection, se for 0 não existe, se for 1 existe. O caracter Z refere-se ao estado do nó leaf, novamente, se for 0 não existe, se for 1 existe. A figura 4.34 representa o formato do pacote enviado entre o XMPP Client e o XMPP Component.

Figura 4.34: Informação trocada entre o XMPP Client e o XMPP Component

O XMPP Component ao receber este pacote analisa o primeiro parâmetro e verifica o valor de X e de Z e caso não existam os respectivos nós, cria-os antes de efectuar a publicação.

4.10.6 Mensagens de Registo

Ao analisar o tipo de mensagens utilizado para estabelecer a ligação pelo protocolo MIH 802.21 verifica-se que não foram utilizadas mensagens de registo. Esta exclusão deve-se ao facto do mecanismo de registo além estar especificado para ser utilizado apenas entre dois MIH Users representa uma forma de implementação de suporte para *accounting* em 802.21 que não é objecto de estudo nesta dissertação. [25]

4.10.7 IEEE 802.15.4 e o 802.21

Uma das alternativas no desenvolvimento deste projecto poderia ter passado pelo desenvolvimento do protocolo 802.21 directamente sobre a tecnologia de rádio utilizada entre os sensores. Esta abordagem não foi utilizada nesta dissertação por dois motivos, o primeiro, o IEEE 802.15.4 é um protocolo que foi desenvolvido com vista às camadas mais baixas, ou seja, camada física e media access control para redes sem fio de baixo débito, ora, uma vez que o objectivo desta dissertação é pode disponibilizar para as camadas mais altas informação de contexto que possa influenciar as aplicações e dispositivos, o desenvolvimento da norma 802.21 neste âmbito seria um pouco infrutífero os objectivos da dissertação. Por outro lado e efectuando uma análise mais abstracta, faz mais sentido que o utilizador não aceda directamente por 802.21 a todos os nós de uma rede, mas sim a um nó eleito, minimizando o *flooding* de informação na rede e a obtenção de dados pouco exactos.

Capítulo 5

Avaliação do Protótipo

5.1 Resultados Experimentais

Após o desenvolvimento do protótipo verificou-se o funcionamento com os três equipamentos já referidos, o desktop, laptop e netbook.

5.1.1 Condições de Teste

Os três equipamentos utilizados encontravam-se a correr no sistema operativo Ubuntu Linux versão 9.10 com ligação LAN por Ethernet e interligação conseguida através de um *switch* local com atribuição de IP por servidor DHCP.

5.1.2 Equipamentos

Descrevem-se de seguida as características físicas dos equipamentos utilizados.

Equipamento	**Nome**	**Descrição**
Desktop	Gateway 802.21	Hardware: Torre Asus Intel Pentium 4 1GB de RAM Placa de Rede RealTek 100MB
Laptop	Utilizador Publicador	Hardware: Macbook Intel Core 2 Duo - 2.4 GHZ 2GHz de RAM Placa de Rede NVIDIA MCP79-1
Netbook	Utilizador Móvel	Hardware: Asus EeePC 1002HA Intel Atom N270 - 1.60GHz 1GB de RAM Placa de Rede Atheros AR8121

5.1.3 Procedimentos

Conectaram-se os três equipamentos ao *switch* por Ethernet. Após *boot* das máquinas conectaram-se, por USB, os Sun Spots (dispositivos e b*asestation*) ao desktop para se poder dar início à instalação do *software*.

Instalação

Começou-se por fazer o *deploy* do código de sensores para os Sun Spots através do NetBeans. Feita a instalação dos Sun Spots removeram-se os dispositivos da ligação USB deixando apenas conectada a *basestation* uma vez que esta não funciona de outra forma por não ter bateria interna. Após instalação e remoção dos dispositivos estes encontram-se desligados e em *standby*.

No desktop, activou-se o módulo de controlo local dos sensores pelo netbeans, este módulo vigia e recebe a informação dos dispositivos Sun Spots contectados à *basestation* por 802.15.4. Inicialmente não existem dados nem sensores conectados uma vez que os dispositivos se encontram desligados. As MIHFs de cada equipamento são configuradas com os IPs locais dos seus pares uma vez que ainda não dispõem de mecanismos de descoberta de endereços.

Activação do Protótipo

Estando o processo de instalação concluído o protótipo encontra-se pronto para ser iniciado. O primeiro passo a ser efectuado é colocar os dispositivos Sun Spots em modo online. Assim que os dispositivos são ligados, no desktop obtêm-se logo a informação dos sensores ligados e da informação que estão a fornecer. A figura 5.1 é um *printscreen* da janela de monitorização referida.

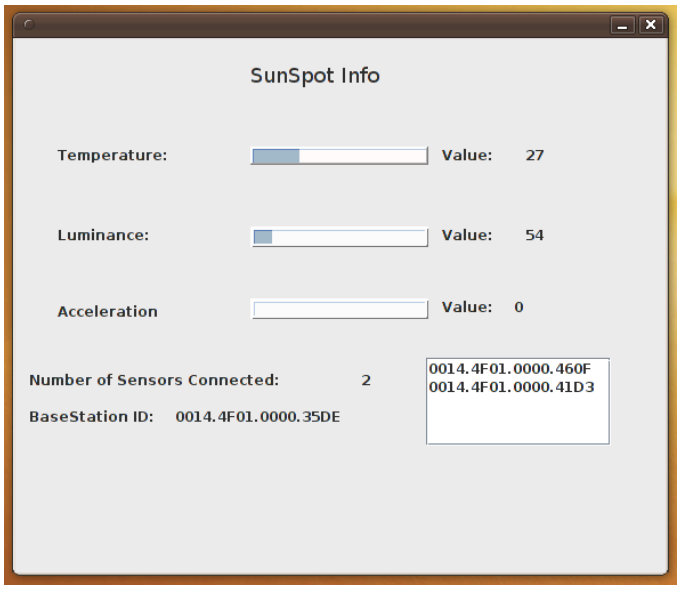


Figura 5.1: Janela de Informação e Controlo de Sensores

A janela graficamente é composta por barras de progresso, uma para cada tipo de sensor, um indicador do número de dispositivos conectados, o MAC ID da *basestation* e os MAC IDs dos dispositivos SunSpots activos.

Antes de colocar online as restantes entidades é necessário configurar a MIH Sensor SAP, do desktop, com o nome do *Collection Node* que se deseja criar no PT Context Broker, sob

a qual será alojado o *Leaf Node* correspondente à informação recolhida pela basestation.

Activaram-se, através da consola do Ubuntu, as MIHFs em cada equipamento para que assim que as entidades, MIH Users e MIH Sensor SAP, comecem a comunicar com a rede as mensagens sejam imediatamente reencaminhadas para o seu destinatário e não hajam perdas.

Iniciou-se a MIH Sensor SAP através do IDE Netbeans e a partir desse instante começou a ser armazenado no módulo colector de informação, os dados de sensores, ao qual a MIH Sensor SAP irá aceder se lhe for pedida essa informação.

No laptop inicia-se o utilizador publicador, que activa o mecanismo de descoberta de capacidades que se difunde por *broadcast*. A *gateway* do desktop irá então responder indicando a informação das capacidades suportadas bem como do endereço do servidor e nó para respectiva publicação. Assim que o utilizador publicador recebe esta informação, efectua o processo de subscrição de eventos e configuração de limiares. Após estes processos estarem concluídos o utilizador publicador do laptop passa a receber a informação que subscreveu e configurou dispondo simultaneamente do mecanismo de Pergunta/Resposta através de mensagens MIH Sensor Action.

A informação recebida é mostrada no monitor do laptop através de uma janela que indica os valores recebidos pelos sensores e imediatamente publicada para o PT Context Broker por XMPP e para o Pachube por HTTP, no entanto, estes processos são transparentes para o utilizador. A figura 5.2 é um *printscreen* da janela de monitorização do utilizador publicador.

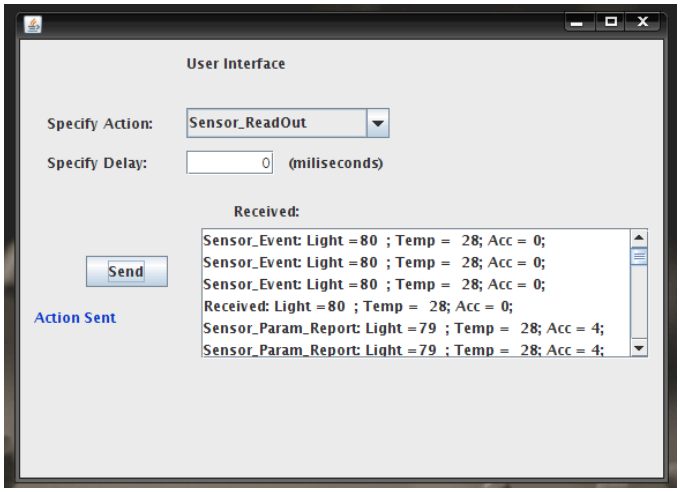


Figura 5.2: Janela de Informação e Controlo de Informação de Contexto

A janela é composta graficamente por uma *listbox* que permite especificar a acção a enviar, neste caso apenas foi utilizada a acção de *Read Out* que permite obter informação dos sensores, uma *editbox* que permite especificar o *delay* com que a acção será executada, um botão "Send"para enviar a mensagem e uma *listview* que mostra todas as mensagens recebidas com informação de contexto. Na imagem podem ser identificadas três tipos de mensagens diferentes, as notificações de subscrição (Sensor Event), as notificações de limiares transpassados (Sensor Param Report) e a reposta à mensagem MIH Sensor Action (Received).

Cenário 1 - Funcionamento

Neste cenário o utilizador móvel irá consumir informação de contexto através da extensão para sensores do protocolo MIH 802.21.
O MIH User do utilizador móvel, no netbook, começa por difundir, por *broadcast*, a mensagem do mecanismo de descoberta. Quando a MIH Sensor SAP detecta este mecanismo despoleta, no desktop, apenas para efeitos de teste, uma janela *pop up*, perguntando qual o tipo de suporte (directo por 802.21 ou através de um *context broker* remoto) a fornecer ao utilizador móvel. Para este cenário escolheu-se o suporte directo, fornecendo a informação de contexto através das mensagens de extensão para sensores do protocolo MIH 802.21. A figura 5.3 é um *printscreen* da janela *pop up* de decisão quanto ao meio de acesso suportado demonstrando a escolha do suporte directo para o transporte de informação de contexto por 802.21 conseguida através do botão "*Direct Suport*".

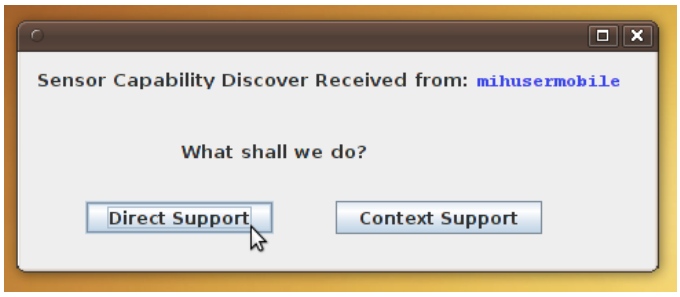


Figura 5.3: Janela de Decisão do Meio de Acesso Suportado pela Gateway

Ao mecanismo de descoberta segue-se o mecanismo de subscrição. Assim que se garante que o mecanismo de subscrição foi concluído com sucesso é mostrado ao utilizador uma janela com a informação dos sensores e que mensagem forneceu esses dados. A figura 5.4 é um *printscreen* da janela de monitorização do utilizador móvel.

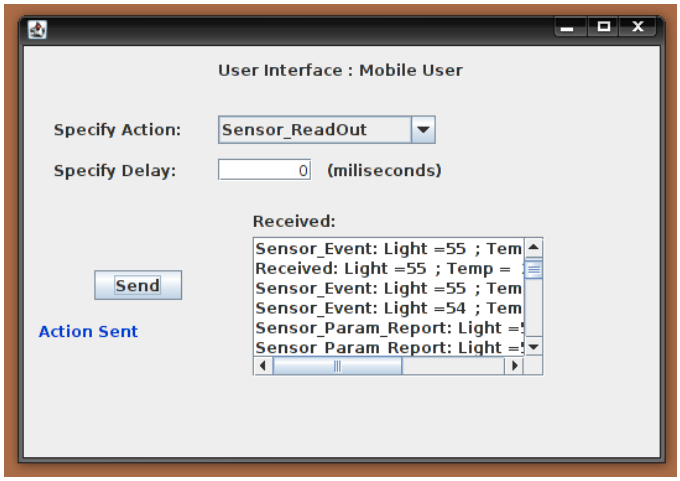


Figura 5.4: Janela de Informação e Controlo de Informação de Contexto do Utilizador Móvel

Esta janela é semelhante à janela de monitorização usada pelo utilizador publicador.

Cenário 2 - Funcionamento

Neste cenário o utilizador móvel irá aceder a informação de contexto através do protocolo XMPP consumindo informação pelo servidor XMPP PT Context Broker.

O MIH User do utilizador móvel, no netbook, difunde por *broadcast* a mensagem do mecanismo de descoberta. No desktop, desta vez, é informada a MIH Sensor SAP que deve responder que não suporta ligação à informação de contexto directamente por 802.21 mas que a informação pode ser obtida através do PT Context Broker e do nó configurado para esse fim. O utilizador móvel assim que recebe esta informação, desliga-se do protocolo 802.21 e utiliza o protocolo XMPP para contactar o PT Context Broker e subscrever o nó de informação de contexto.A figura 5.5 é um *printscreen* da janela *pop up* de decisão quanto ao meio de acesso suportado.

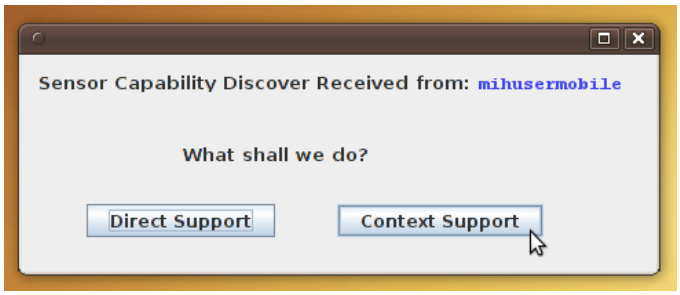


Figura 5.5: Janela de Decisão do Meio de Acesso Suportado pela Gateway

A imagem demonstra a escolha do suporte directo para o transporte de informação de contexto por XMPP conseguida através do botão "Context Suport".

Assim que obtém ligação e completada a subscrição é mostrado ao utilizador uma janela indicando o endereço do servidor e a informação sobre os dados dos sensores que vai sendo actualizada. A figura 5.6 é um *printscreen* da janela de monitorização do utilizador móvel.

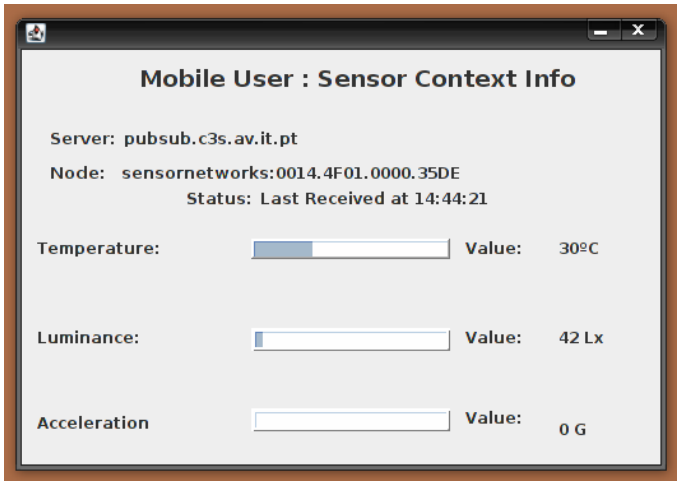


Figura 5.6: Janela de Informação e Controlo de Informação de Contexto do Utilizador Móvel

A janela descreve o endereço do servidor como sendo o "pubsub.c3s.av.it.pt"que corresponde ao PT Context Broker e indica o nó subscrito. O Collection Node é o sensornetworks e a leaf é sensornetworks:0014.4F01.0000.35DE. Na janela é indicado também a hora de recepção da ultima mensagem de actualização bem como as barras de progresso que indicam os valores recolhidos pelos sensores e disponibilizados pelo PT Context Broker.

Informação no Pachube

A plataforma pachube foi bastante útil no desenvolvimento do protótipo pois permitiu armazenar e organizar a informação *online* ao mesmo tempo que disponibiliza ferramentas para acesso aos dados por localização través do Google Maps. Desta forma foi possível acompanhar o desenvolvimento e o sucesso da publicação bem como a consistência dos dados disponibilizados.

A imagem 5.7 mostra um *printscreen* obtido do site Pachube com os dados referentes à localização desta prova de conceito através do Google Maps embutido no *website*.

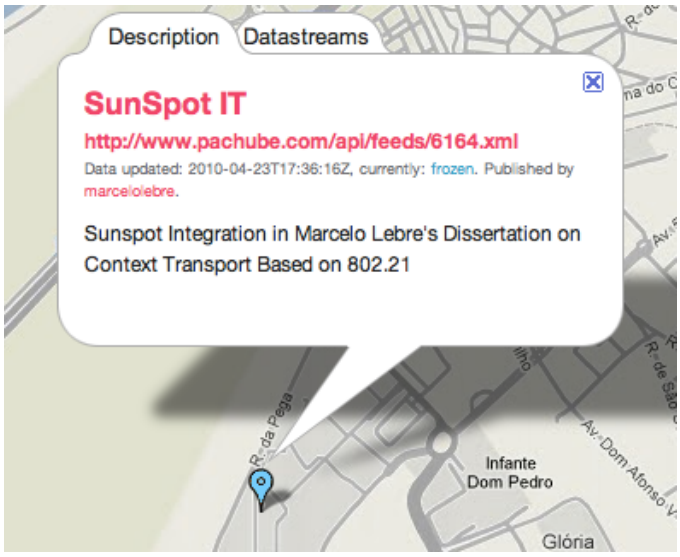


Figura 5.7: Localização de Sensores com Google Maps Pachube

Esta dissertação, bem como a prova de conceito, participam no enriquecimento e divulgação da plataforma Pachube que aspira a ser um sistema de centralização e disponibilização de informação de contexto a uma escala global. A plataforma merece todo o mérito pelo seu tema e ambição "*patching the earth*"e pelos vários meios que disponibilizam, além de existirem bibliotecas para o desenvolvimento de *software* num grande número de linguagens, existe também suporte para aplicações em plataformas móveis como Iphone OS e Android.

A biblioteca Pachube Java utilizada na implementação desenvolvida além de bastante bem documentada a sua utilização para aceder aos serviços da plataforma pode ser conseguida de forma bastante fácil e rápida.

Informação no PT Context Broker

Como já explicitado, a informação no PT Context Broker está estruturada na forma de *Leaf Nodes* alojados em *Collection Nodes*. A figure 5.8 é um *printscreen* da estrutura interna da organização dos nós.

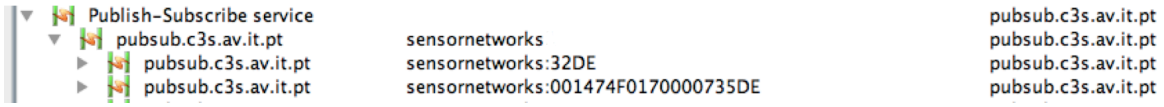


Figura 5.8: Localização de Sensores com Google Maps Pachube

A imagem apresentada foi retirada com um cliente XMPP que permite aceder ao serviço de descoberta e analisar os serviços disponibilizados pelo servidor XMPP. Após expandir o serviço de PubSub pode-se verificar o collection node sensornetworks com os vários leaf nodes de teste associados.

5.2 Análise de Bibliotecas XMPP

As bibliotecas Java utilizadas no desenvolvimento dos elementos XMPP, *Context Consumer* e *Context Provider*, nesta dissertação possibilitam que seja feita uma caracterização da sua utilização e desempenho.

5.2.1 Smack

Smack é uma biblioteca Java *open source* para a criação de clientes XMPP com suporte a mensagens instantâneas e mensagens de presença. Permite o desenvolvimento desde clientes XMPP com todas as funcionalidades que lhe são inerentes a aplicações de envio de mensagens de notificação.

5.2.2 Whack

Whack é uma biblioteca Java *open source* para componentes XMPP. Esta biblioteca apresenta uma flexibilidade no desenvolvimento de software dado que tanto permite criar um componente XMPP completo como apenas uma integração XMPP com uma aplicação já existente para interceptar e agir mediante recepção de certas mensagens.

5.2.3 Tinder

Tinder é uma biblioteca XMPP para a linguagem Java que fornece suporte para stanzas e componentes XMPP. Esta biblioteca deriva da previa implementação da biblioteca Whack bem como do *software* Openfire da Jive.

5.2.4 Comparação

Na criação do cliente XMPP do Context Consumer a biblioteca Smack desempenhou o seu papel na sua perfeição, no entanto, na criação do componente XMPP do *Context Provider* a biblioteca Tinder demonstrou alguns *bugs* de implementação ao nível de *handlers* de recepção de mensagens de resposta a *stanzas* de *query* a nós. Após pesquisa na documentação

e plataforma de desenvolvimento *online* da Smack, encontrou-se documentação sobre os mesmos *bugs*. Estes *bugs* apresentam um reporte de ha já vários meses e até à data não foram resolvidos. A justificação encontrada por alguns *developers* prende-se com o facto do código da biblioteca Tinder ter simplesmente migrado da biblioteca Whack para esta sem grandes adaptações.
No desenvolvimento do *Context Provider*, encontrou-se outro problema com a biblioteca Tinder no auxílio à construção de pacotes IQ com suporte de mecanismo PubSub. Esta questão foi resolvida incluindo no mesmo projecto a biblioteca Whack como suporte a algumas funcionalidades que a biblioteca Tinder não suporta.

Concluindo a análise das bibliotecas utilizadas, no desenvolvimento de clientes XMPP a biblioteca Smack apresenta já algum grau de maturação e robustez enquanto que para desenvolver componentes XMPP é aconselhável utilizar a biblioteca Tinder para o exoesqueleto do componente e complementar as funcionalidades com recurso à biblioteca Whack.

5.3 Mensagens

Analisaram-se os tamanhos das mensagens de extensão para sensores do protocolo MIH 802.21 bem como as mensagens utilizadas para estabelecer a publicação e o consumo de informação por XMPP. As tabelas 5.1 e 5.2 representam os tamanhos de cada mensagem utilizada para cada respectivo cenário. De relembrar que, no primeiro cenário o utilizador móvel consome a informação pelo protocolo MIH 802.21 com a extensão para sensores do 802.21 e no segundo cenário o utilizador consome a informação por XMPP.

Mensagens MIH 802.21

Mensagem	**Cenário**	**Tamanho (Bytes)**
MIH_Sensor_Capabilities_Discover.Request	1, 2	39
MIH_Sensor_Capabilities_Discover.Response	1, 2	50
MIH_Sensor_Capabilities_Discover.Response	2	98
MIH_Sensor_Event_Subscribe.Request	1, 2	71
MIH_Sensor_Event_Subscribe.Response	1, 2	30
MIH_Sensor_Configure_Thresholds.Request	1, 2	63
MIH_Sensor_Configure_Thresholds.Response	1, 2	30
MIH_Sensor_Event.Indication	1, 2	54
MIH_Sensor_Parameter_Report.Indication	1, 2	54
Continua na próxima página		

Tabela 5.1 – Continuado a partir da página anterior

Mensagem	Cenário	Tamanho (Bytes)
MIH_Sensor_Action.Request	1, 2	40
MIH_Sensor_Action.Response	1, 2	55

Tabela 5.1: Tamanho das Mensagens MIH 802.21Utilizadas

Mensagens XMPP

Mensagem	Cenário	Tamanho (Bytes)
PubSub - Discover Node Info	1, 2	125
PubSub -Create Collection Node	1, 2	446
PubSub -Create Leaf Node	1, 2	317
PubSub - Publish	1, 2	400
PubSub - Subscribe	2	215
PubSub - Update	2	200

Tabela 5.2: Tamanho das Mensagens XMPP Utilizadas

Como se pode visualizar, nas tabelas estão representados três campos, o campo mensagem que indica a designação da mensagem referente ao protocolo, o campo cenários que indica em que cenários a mensagem é utilizada e o campo tamanho, que indica, respectivamente a cada cenário o tamanho da mensagem.

5.3.1 Utilização da Rede

Após efectuar algumas experiências com o protótipo e visualizar o seu funcionamento, o sucesso da prova de conceito quanto à implementação inicial deu lugar a questões na áreas de escalabilidade e sobrecarga na rede. Para este efeito efectuaram-se alguns cálculos a fim de visualizar o impacto da utilização efectiva deste conceito numa rede com vários utilizadores/equipamentos.

Considere-se o seguinte quanto a mensagens de extensão para sensores do protocolo MIH 802.21 num pior caso onde todas as mensagens trocadas possuem tamanho igual ao maior

tamanho de mensagens existente, 98 bytes. Existe, numa situação normal um processo inicial para descoberta, seguido do processo de subscrição e do processo de configuração. Cada processo requer duas mensagens, uma de *reques* e uma de response para se considerarem bem sucedidos. Concluídos estes processos, assume-se num caso de extrema utilização que o processo de subscrição configura uma periodicidade de um segundo, significa isto que serão enviadas mensagens MIH_Sensor_Event a cada segundo e que o processo de configuração específica limiares extremamente perto dos valores de oscilação normal dos sensores e existe um transpassamento destes valores em metade do tempo de medição. Além destas especificações, assume-se também que o utilizador questiona de dois em dois segundos o estado dos sensores através da mensagem MIH_Sensor_Action, que implica duas mensagens, uma de *request* e outra de response. Pode-se calcular separadamente a carga inicial criada pelos processos de descoberta, subscrição e configuração e uma carga secundária criada pela troca contínua de mensagens com duração de uma hora para um utilizador. Colocando todo este enunciado em formato matemático obtém-se:

M -Tamanho da mensagem.
Ct - Carga total.
Cc - Carga contínua.
Ci - Carga Inicial.
T - Tempo de experiência (Segundos).
Ts - Periodicidade subscrita (Segundos).
N - Número de execuções.
Nc - Número de transpassamentos de limiares ocorrido.
Npr - Número de vezes executado o mecanismo Pergunta/Resposta.
Pd - Número de transpassamentos de limiares ocorrido.
Ps - Número de transpassamentos de limiares ocorrido.
Pc - Número de transpassamentos de limiares ocorrido.

$$\mathbf{Ci} = [\mathbf{Pd} \times \mathbf{N} + \mathbf{Ps} \times \mathbf{N} + \mathbf{Pc} \times \mathbf{N}] \times \mathbf{M} \tag{5.1}$$

Substituindo, Pd = 2, N = 1 e M = 98 obtém-se:

$$\mathbf{Ci} = 588 \tag{5.2}$$

O próximo passo é calcular a carga na rede criada pela troca contínua de mensagens. Neste passo, é importante especificar um período de tempo para calcular a carga imposta na rede pelas mensagens e extrapolar as suas consequências. Novamente, colocando em formato matemático:

$$\mathbf{Cc} = [\mathbf{T}/\mathbf{Ts} + \mathbf{Nc} + \mathbf{Npr}] \times \mathbf{M} \tag{5.3}$$

Substituindo, T = 3600, Ts = 1, Nc = 1800, Npr = 1800, M = 98 obtém-se:

$$\mathbf{Cc} = 705600 \tag{5.4}$$

Finalmente, calculando a carga total:

$$\mathbf{Ct} = \mathbf{Ci} + \mathbf{Cc} \tag{5.5}$$

Substituindo Ci = 588 e Cc = 705600, obtém-se:

$$\mathbf{Ct} = 706188 \tag{5.6}$$

Ao longo de uma hora de troca de mensagens obtém-se uma carga na rede de cerca de 706188 Bytes, ou seja, aproximadamente 690KB. Pode-se então, efectuar uma verificação da taxa de ocupação da ligação para uma hora mediante as capacidades de cada tecnologia através da tabela 5.3.

Mensagem	**Cenário**	**Tamanho (Bytes)**
UMTS	384Kbps	0.05%
3G	3.6 Mbps	0.005%
3G	7.2 Mbps	0.0025%
WiFi - 802.11g	24 Mbps	0.0008 %
WiMAX	75 Mbps	0.00024 %
Ethernet	100 Mbps	0.00011 %

Tabela 5.3: Tabela de Ocupação de Ligação

5.3.2 Escalabilidade

Existem dois parâmetros sobre os quais se podem recair as considerações sobre escalabilidade num sistema estruturado segundo a arquitectura proposta, a escalabilidade quanto ao número de utilizadores mediante taxa de ocupação da rede e a escalabilidade quanto ao número de utiizadores mediante sobrecarga nos serviços de informação e *gateway* de sensores.

O impacto da ocupação da rede originado pelo número de utilizadores com suporte de mensagens com expansão para sensores do protocolo MIH 802 pode ser analisado pela gráfico da imagem 5.9.

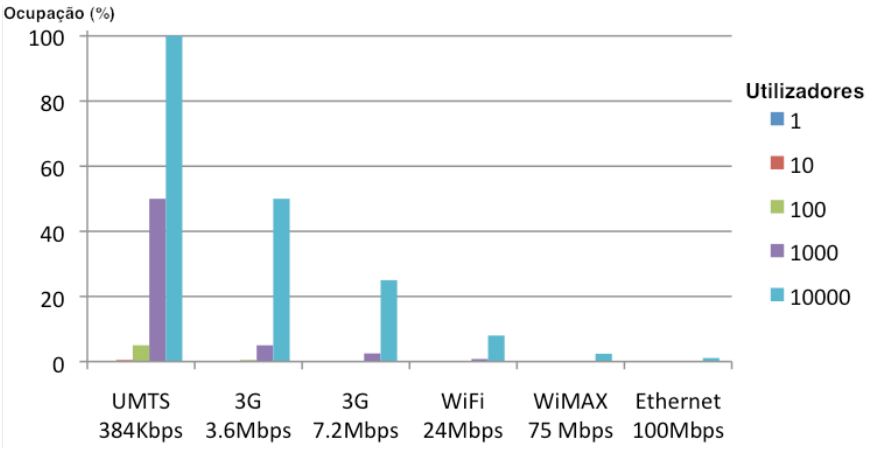


Figura 5.9: Gráfico de Ocupação por Número de Utilizadores

Como se pode verificar pelo gráfico, a utilização deste tipo de solução só se torna crítica para valores bastante altos (>5000) de número de utilizadores e apenas com tecnologias que apresentem largura de velocidades iguais ou inferiores a 3.6 Mbps (UMTS e 3G). Por outro lado, todas as outras tecnologias, apresentaram uma taxa de ocupação aceitável e o seu impacto na rede não é substancial.

De notar que, este exemplo foi considerado para uma utilização intensiva para cada utilizador, situação que não ocorrerá com facilidade dada a efemeridade da ligação que cada utilizador móvel tem na realidade com uma rede.

Embora não tenha sido efectuado um estudo sobre a escalabilidade do ponto de vista de gestão de recursos computacionais, pode-se, inferir, que o protocolo não efectua uma utilização extensiva da ligação e da rede pelo que se torna, comparando os seus beneficios em detrimento do peso computacional e de rede, perfeitamente utilizável. Quanto às mensagens do protocolo XMPP, não se torna necessário demonstrar um estudo quanto à sua utilização uma vez que é um protocolo já com provas dadas nos vários âmbitos da sua utilização. [26]

5.4 Medidas de Sensores

Não foi implementado, durante o desenvolvimento da prova de conceito, um mecanismo de histórico para os dados obtidos através dos dispositivos Sun Spots uma vez que não fazia parte do contexto desta dissertação estudar em pormenor os valores obtidos por dispositivos sensoriais. No entanto, e beneficiando da versatilidade da plataforma Pachube, foram gerados, automaticamente, gráficos com um histórico de evolução temporal de cada um dos tipos dados registados no *feed* criado. A figura 5.10 é um printscreen dos gráficos referidos.

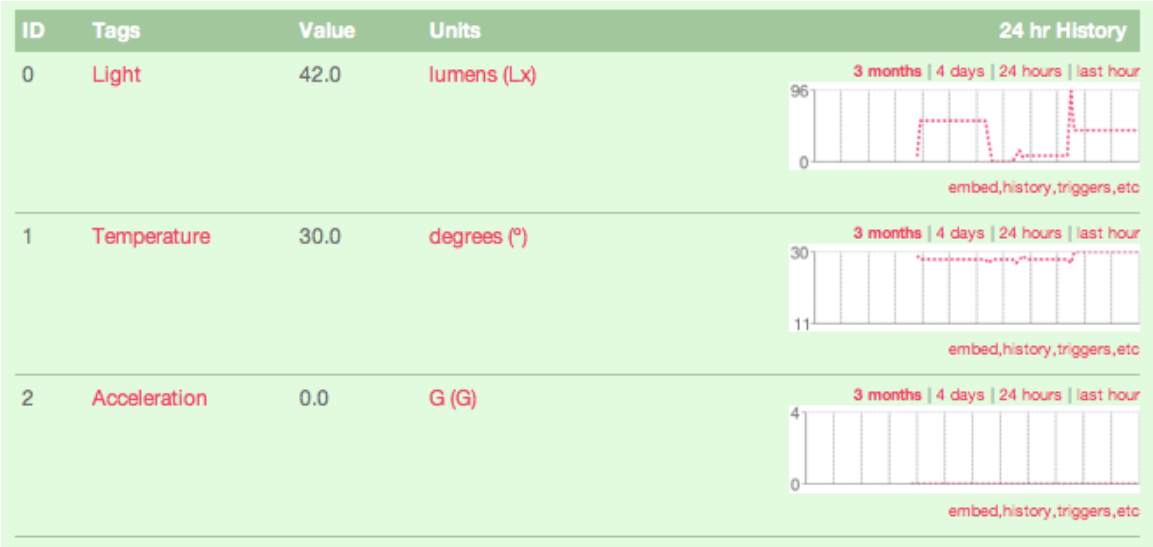


Figura 5.10: Interface Grafica Google Maps do Pachube

Os dados reflectidos pelos gráficos representam apenas amostras de dados retiradas ao longo dos testes com os sensores e encontram-se numa escala temporal que abrange um histórico de três meses. Na coluna *Value* encontram-se os valores actuais dos sensores, na coluna *Units* encontram-se as unidades utilizadas nas medições, na coluna *Tags* encontra-se o nome utilizado para caracterizar o tipo de sensor e o ID representa a identificação do sensor no feed.

5.5 Disseminação

O trabalho realizado nesta dissertação constitui base para um conjunto de artigos que se encontram em elaboração. Nestes artigos pretende-se evoluir o trabalho apresentado, focando questões de interfaces para sensores em contextos mais genéricos potenciando cenários de mobilidade e interacção com várias tecnologias de comunicações sem fios.

Capítulo 6

Conclusões

Nesta dissertação foi, inicialmente, apresentada uma arquitectura para o transporte de contexto baseado no protocolo MIH da norma 802.21 com suporte alternativo recorrendo a serviços de informação demonstrando a integração das três áreas tecnológicas, redes de sensores, redes heterogéneas e plataformas de gestão de contexto. Demonstrou-se uma proposta para a extensão de suporte sensores do protocolo MIH 802.21 com base no transporte de informação de contexto integrando as redes de sensores, sua organização e vantagens para a contextualização de dados, com os serviços de informação, permitindo o suporte e acesso aos dados para os mais variados fins.

Apresentou-se a prova de conceito, construída em parceria com os projectos ODTONE e PT Context Broker, confirmando a validade da arquitectura proposta e permitindo simultaneamente o desenvolvimento de um protótipo com vista ao transporte contexto com base no protocolo 802.21 fazendo uso de um serviço de informação através dum servidor XMPP como repositório de dados para acesso alternativo. Foi demonstrado o funcionamento do protótipo em dois cenários variando o método de acesso à informação mantendo sempre por base a utilização de mensagens de extensão para sensores do protocolo MIH 802.21 e o seu sucesso demarcou a validação da prova de conceito elaborada como suporte para futuros projectos/artigos.

As redes de sensores SunSpots provaram ser uma fonte de informação importante na caracterização do ambiente envolvente, fornecendo dados sobre várias medidas que podem influenciar o funcionamento de uma rede ou a interacção de um utilizador com a ligação. Conseguiu-se também concluir como o protocolo 802.21 pode ser útil na gestão de endereços ip recorrendo à camada L2,5.

O protocolo XMPP e as suas entidades tornaram-se um elo de ligação importante tornando evidente as vantagens da sua utilização forma de acesso a informação alternativa. O PT Context Broker permitiu a convergência de informação a distribuir para os utilizadores dando a conhecer a sua versatilidade para agregação e disponibilização de informação como Context Broker.

A implementação do protótipo demonstrou as capacidades do protocolo 802.21 não só como protocolo que potencia o *handover* mas como tirar partido da camada L2,5, onde opera,

facilitando o acesso à informação de contexto sem necessitar autenticação L3. O desenvolvimento de todo o protótipo em Java revela a interoperabilidade e diversifica os cenários de instalação da prova de conceito.

A avaliação do protótipo exemplificou como a utilização deste tipo de mensagens pode ser aplicável a uma rede e com os impactos nas diversas tecnologias. Foi efectuada uma breve análise de bibliotecas XMPP disponíveis para a linguagem Java explicitando os seus pontos fortes e fracos quando inseridos no protótipo apresentado. Utilizou-se também como foi utilizado o *webservice* Pachube e as suas funcionalidades para suporte ao desenvolvimento da prova de conceito.

Na secção seguinte serão apresentadas algumas aplicações práticas e casos de uso que reflectem a arquitectura proposta nesta dissertação.

6.1 Trabalho Futuro

Durante a elaboração da prova de conceito foram surgindo algumas ideias e iniciativas que promovem a evolução deste protótipo em várias direcções. Algumas dessas considerações podem ser apresentadas como trabalho futuro nas três áreas tecnológicas abrangidas por esta dissertação.

6.1.1 Sistema de Informação para Sensores baseado em 802.21

Na prova de conceito apresentada, foi utilizado um sistema de informação externo ao protocolo MIH 802.21 e para o controlo e obtenção de informação foram utilizados os serviços de eventos e comandos da extensão para sensores do protocolo MIH 802.21. O que se propõe para um trabalho futuro é a integração, neste protótipo, de um sistema de informação extendido para sensores do protocolo MIH 802.21. Este mecanismo permitirá o acesso directo de informação de contexto não dependendo unicamente de um servidor externo para o armazenamento e disponibilização de informação.

No protótipo implementado, utilizando a extensão para sensores do protocolo MIH 802.21 apenas se pode aceder a informação de contexto actual, ou seja, não existe, nesta camada forma de aceder aos dados anteriores à ultima actualização. Esta sugestão tem como objectivo disponibilizar um histórico de informação inteiramente ao nível L2,5 através do serviço de informação (MIIS).

O recurso a este serviço (MIIS) retira algum peso de computação e encaminhamento ao serviço de comandos e eventos, uma vez que o acesso à informação pode, agora, também ser feito efectuado por outro serviço. A publicação dos dados, pode continuar a ser efectuada pelo MIH User do utilizador publicador, todavia, não só publica para um servidor remoto através de outro protocolo, publica também para a base de dados do serviço de informação por uma mensagem do tipo *push* para inserção dos dados. Os MIH Users dos utilizadores móveis podem aceder à informação através de uma mensagem do tipo *pull* para obtenção dos dados.

6.1.2 Redes de Sensores Adaptativas

As redes de sensores utilizadas neste protótipo apresentam um funcionamento pouco dinâmico do ponto de vista de gestão energético e recuperação de falhas uma vez que saía fora do âmbito da dissertação. Tendo em conta este aspecto, propõe-se algumas modificações no funcionamento da rede de sensores ao nível do nó e ao nível da organização de nós que compõe a rede de sensores.

Individualmente, propõe-se que cada nó da rede de sensores faça uma gestão interna da energia conciliando o estado da sua bateria com o seu funcionamento. Esta adaptação pode ser conseguida regulando as medições efectuadas pelos sensores com a intensidade dos pedidos à rede de sensores. Se a rede de sensores receber poucos pedidos, as leituras efectuadas pelos sensores podem ser pausadas ou podem mesmo ser desligados alguns sensores quando não existam pedidos.

Para organização da rede de sensores propõe-se o comando individual de cada nó consoante a sua posição na rede, os sensores que possui agregados e o tempo de resposta. Se uma rede de sensores for vasta, então ao utilizador pode interessar mais as medidas dos sensores que se encontram mais perto, para este efeito a rede não precisa de requisitar a informação de todos os nós, poupando bateria e tempo de encaminhamento da informação. Cada nó pode possuir vários sensores agregados (e.g. luz, temperatura, humidade, ruído, etc.), se um utilizador pedir informação sobre temperatura, não faz sentido questionar todos os nós sobre esta medida, basta apenas questionar os nós que possuírem os sensores dos quais se quer obter informação. Relativamente ao tempo de resposta, assume-se que todos os nós possam possuir capacidades de computação diferentes, por este motivo, o atraso em alguns segundos de uma leitura pode invalidar o calculo da media ou estado dos sensores num dado momento, por este motivo convém ter em conta os tempos de resposta dos nós e o impacto que possa ter na performance da rede de sensores.

6.1.3 Desenvolvimento de MIHF Ciente de Contexto

A MIHF utilizada no protótipo não está internamente estruturada para lidar com as mensagens da expansão para sensores do protocolo MIH 802.21, delegando a responsabilidade e alguns mecanismos para as entidades imediatamente a cima e a baixo de si (e.g. MIH Sensor Sap, MH User).

A proposta apresentada é no sentido de dotar a MIHF de mecanismos para reconhecimento e controlo de subscrições, configurações e fluxo de mensagens MIH 802.21 para sensores. O mecanismo para controlo de subscrições pode auxiliar para regular a selecção de eventos possibilitando atribuir os vários tipos de eventos aos vários tipos de utilizadores separando a sua utilização e ao mesmo tempo regulando também a periodicidade mínima e máxima permitida para a recepção de notificações. O mecanismo de controlo de configurações auxilia a verificação dos utilizadores que possam ou não configurar limiares de transpassamento conciliando os recursos disponíveis pela *gateway* onde se encontra a MIHF e as permissões do MIH User. Por fim, o mecanismo de controlo do fluxo de mensagens serviria para impedir que existissem situações de congestionamento da rede pelas mensagens de informação de contexto,

este mecanismo actuaria em conjunto com outro sub mecanismo de QoS garantindo que a experiência dos utilizadores não será prejudicada pela errónea utilização de mensagens de extensão para sensores do protocolo MIH 802.21.

6.2 Transporte de Contexto baseado em 802.21 no ODTONE e PT Context Broker

Ao longo da dissertação foi essencial a colaboração simbiótica com os projectos ODTONE e PT Context Broker.
O desenvolvimento do protocolo MIH 802.21 em Java resultante desta dissertação incorporará uma futura *release* do ODTONE provando a sua interoperabilidade entre sistemas. Possibilitou ainda, ao longo do estudo do trabalho já efectuado, ajudar na detecção e reparação de pequenos *bugs* no *software* já existente do ODTONE.
Quanto ao projecto PT Context Broker, a utilização de sensores como os Sun Spots demonstrou ter lugar no PT Context Broker como sendo uma das fontes de informação de contexto que no futuro será utilizada para caracterizar informação e apoiar a tomada de decisões baseadas em contexto.

O desenvolvimento emparelhado com estes projectos permitiu a esta dissertação beneficiar da experiência acumulada nas várias áreas e obter proveito do conhecimento já reunido pelos projectos em causa.

6.3 Considerações Finais

O desenvolvimento desta dissertação e de toda a inerente implementação, possibilitou a aprendizagem aprofundada nas três áreas tecnológicas abordadas.
Sobre as redes de sensores, a utilização da tecnologia Sun Spot revelou-se uma abordagem inovadora e orientada ao desenvolvimento de nós de redes de sensores. As funcionalidades e facilidades trazidas à área por estes dispositivos, impulsionaram certamente a evolução das funcionalidades e capacidades dos nós de sensores.
As redes heterogéneas têm um papel preponderante nesta dissertação, revelando-se uma positiva caixa de pandora no que diz respeito às possibilidades, capacidades e potencialidades que facilita. Sendo um tema em constante evolução e adaptação, as redes heterogéneas beneficiam grandemente deste ponto comum entre as diversas tecnologias que a compõe, que é o protocolo MIH 802.21. A extensão para sensores deste protocolo demonstra a versatilidade e utilidade do facto de operar ao nível L2,5 facilitando a construção de uma camada de inteligente não necessitando de ligação ao nível L3, com todas as vantagens que desta característica advêm.
As plataformas de gestão de informação de contexto demonstra uma solução para a disponibilização, gestão e armazenamento de tanta informação de contexto que circula na rede. É importante a agregação e caracterização dessa informação para permitir a contextualização dos dados e dos utilizadores em prole de serviços que se baseiem no contexto para disponibilizar e potenciar as suas funcionalidades.

A integração das áreas e tecnologias apresentadas concedeu à dissertação utilidade junto dos projectos ODTONE e PT Context Broker ao mesmo tempo que poderá servir de base

para futuros projectos ou artigos. Demonstrou, também, que essa integração facilita a convergência de informação, serviços e experiência de utilização num âmbito que revelará no futuro ser uma mais valia no paradigma das comunicações e equipamentos móveis.

Como considerações pessoais, salienta-se o facto desta dissertação conferir ao autor uma noção de sucesso pelas metas atingidas na criação de uma prova de conceito totalmente funcional e útil. O envolvimento com os projectos e colaboradores associados contribuiu bastante para a formação pessoal e amadurecimento desta prova de conceito durante o seu desenvolvimento. O conhecimento reunido pela investigação na implementação de todo este projecto foi explanado e explicitado ao longo desta dissertação, no entanto, o maior contributo considera-se ter sido para a formação pessoal e profissional do autor.

Bibliografia

[1] IEEE 802.21, "IEEE Standard for 802.21 Media Independent Handover Services," 2008.

[2] Diogo Gomes, Rui Aguiar, "Quasi-omniscient Networks: Scenarios on Context Capturing and New Services Through Wireless Sensor Networks," 2008.

[3] Thomas Strang, Claudia Linnhof-Popien, Matthias Roeckl, "Highlevel Service Handover through a Contextual Framework," 2006.

[4] Paolo Bellavista, Marcello Cinque, Domenico Cotroneo, Luca Foschini, "Integrted Support for Handoff Management and Context Awareness in Heterogeneous Wireless Networks," 2005.

[5] Wei Li, "A Service Oriented SIP Infrastructure for Adaptive and Context-Aware Wireless Services," 2003.

[6] Christian Dannewitz, Stefan Berg, Holger Karl, "An IEEE 802.21-based Universal Information Service," 2006.

[7] Yongguang Zhang, Harrick Vin, Lorenzo Alvisi, Wenke Lee, Son K. Dao, "Heterogeneous Networking: A New Survivability Paradigm," 2002.

[8] Jos Akhtman, "Heterogeneous Networking: An Enabling Paradigm for Ubiquitous Wireless Communications," 2009.

[9] Marc Danzeisen, Torsten Braun, Isabel Steiner, "On the benefits of heterogeneous networking and how cellular mobile operators can help," 2005.

[10] Hiroshi Sakakibara, Jin Nakazawa, Hideyuki Tokuda, "PBN: A seamless Network Infrastructure of Heterogeneous Network Nodes," 2009.

[11] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A Survey," 2001.

[12] Marluce P. , Cláudio A., Maria C., "Tutorial sobre Redes de Sensores," 2003.

[13] S. Tilak, N.B. Abu-Ghazaleh e W. Heinzelman, "A taxonomy of wireless micro-sensor network models," 2002.

[14] Anind K. Dey, Gregory D. Abowd, "Towards a Better Understanding of Context and Context-Awareness," 2000.

[15] Bill N. Schilit, Norman Adams, Roy Want, "Context-aware computing applications," 1994.

[16] Guanling Chen, David Kotz, "A Survey of Context-Aware Mobile Computing Research," 2000.

[17] Gregory Abowd, Maria Ebling, Guerney Hunt, Hui Lei, Hans Gellerson, "Context-Aware Computing," 2002.

[18] RFC3920, "Extensible Messaging and Presence Protocol (XMPP) Core - RFC 3920," 2004.

[19] RFC3921, "XEP-0114: Jabber Component Protocol," 2005.

[20] RFC2277, "IETF Policy on Character Sets and Languages," 2000.

[21] XEP0060, "XEP-0060: Publish-Subscribe," 2005.

[22] Ignite Realtime, "Whack," 2008. [online] `http://www.igniterealtime.org/projects/whack`.

[23] Ignite Realtime, "Tinder," 2010. [online] `http://www.igniterealtime.org/projects/tinder`.

[24] Ignite Realtime, "Smack," 2008. [online] `http://www.igniterealtime.org/projects/smack`.

[25] IEEE 802.21, "IEEE 802.21 MIH Registration," 2008.

[26] Peter Saint-Andre, "XMPP: Lessons Learned from ten yers of XML Messaging," 2009.

[27] SunMicrosystems, "Sun Spot World." Sun Labs. [online] `http://www.sunspotworld.com`.

[28] Connected Environments, "Documentação da API do Pachube." Pachube. [online] `http://community.pachube.com/api`.

Appendices

Apêndice A

ODTONE

A.1 ODTONE - Open Dot Twenty ONE

A.1.1 Apresentação

ODTONE é um projecto integrado na área de redes heterogéneas do Instituto de Telecomunicações Polo de Aveiro e apresenta-se como sendo uma implementação *open source* de uma MIH Function para o *standard* IEEE 802.21 *Media Independent Handover* e subsequentes APIs MIH.

A.1.2 Funcionalidades

Esta implementação de uma MIHF visa o suporte aos serviços inerentes a este elemento, MICS, MIES e MIIS bem como os mecanismos que o compõe, descoberta de capacidades, registo MIHF, subscrição de eventos, *etc.*.

Perante esta implementação, o desenvolvimento de um MIH User deve ser simples e requer um conhecimento mínimo sobre as implementações da MIHF e das especificídades próprio protocolo MIH.

Dispõe-se, ao utilizador que implementar os seus elementos, um conjunto de classes para poder receber e enviar comandos, eventos e informação criando assim uma API, envolvendo as operações de mais baixo nível com uma camada de abstracção que permite um desenvolvimento intuitivo e sem esforço.

A interoperabilidade de sistemas é um ponto focado por este projecto pelo que existem opções de compilação para múltiplos sistemas operativos e todos com as mesmas funcionalidades. Sendo os MIH Link SAPs intrinsecamente ligados aos *drivers* do hardware, a sua implementação depende em grande parte do *kernel* do respectivo sistema operativo. Assim, esta implementação não suporta MIH Link SAPs multi-plataforma para cada tecnologia, sendo que cada uma terá de ser implementada de forma independente usando as APIs fornecidas pelo ODTONE.

A.1.3 Objectivos

O principal objectivo deste projecto é fornecer uma MIHF que possa ser utilizada como base para múltiplos cenários de utilização. Possibilita aos utilizadores de implementar MIH SAPs e MIH LINK SAPs conforme as suas necessidades. O ODTONE providencia uma

interface simples e mais flexível para o desenvolvimento de SAPs manipulando mensagens de protocolo MIH e transições de estado.

A.1.4 Extensibilidade e Modularidade

Foi adoptada uma aproximação modular à implementação da MIHF , conseguindo com isto construir cada mecanismo por forma a possibilitar uma fácil extensão dos mesmos ou ainda a substituição de um dado mecanismo por um mais actualizado. Tal como já foi referido, é esperado que os utilizadores construam os seus próprios elementos, que, em conjunto com a MIHF implementada, sirvam os seus propósitos, no entanto, a modularidade teve em conta a extensão de serviços e novos mecanismos.

Suporta a inclusão de novas primitivas sem necessitar de alterar o código existente.

A.1.5 Arquitectura

A entidade lógica MIHF é responsável pela gestão dos serviços prestados e atribuir o acesso dos mesmos a utilizadores e a várias tecnologias de ligação.

Suportando as premissas que compõe a entidade MIHF e as características modulares e de expansão, a figura A.1 ilustra o conceito implementado.

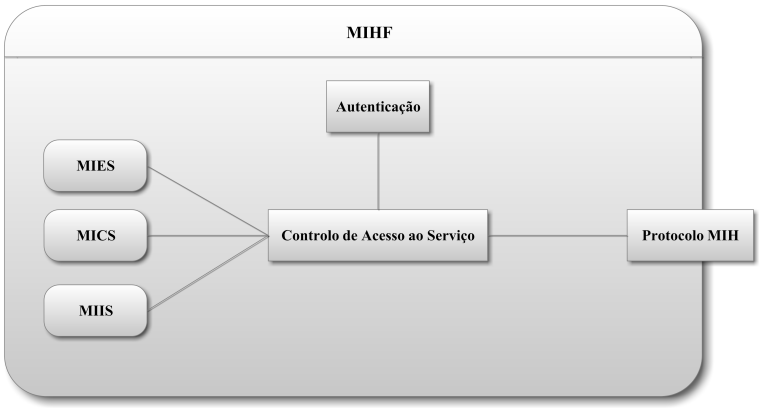


Figura A.1: Submódulos conceptuais MIHF

Quando o módulo Protocolo MIH recebe uma mensagem decompõe-na em estruturas de dados que são enviados para o módulo de Controlo de Acesso ao Serviço(CAS).

O controlo de acesso ao serviço verifica a fonte contida na mensagem e verifica as suas permissões através do módulo de Autenticação para que o utilizador possa ser validado. Esta autenticação permite ao CAS verificar a origem da mensagem e ao mesmo tempo verificar se existem utilizadores registados com interesse na mesma. Após uma validação bem sucedida a estrutura de dados é reencaminhada para o serviço correspondente, MIES, MICS ou MIIS.

O serviço após receber e processar a estrutura de dados retorna uma resposta para o CAS que se encarrega de reencaminhar a mesma ao módulo de Protocolo MIH. O protocolo MIH por fim, transforma a estrutura de dados recebida numa mensagem MIH e despacha-a para o respectivo *socket*. A definição dos módulos encontra-se disponível na especificação de arquitectura do ODTONE.

Apêndice B

SunSpots

SunSpot é um acrónimo para *Sun Small Programmable Object Technology* [27]. É um projecto pertencente à Sun MicroSystems com origem nos Sun Labs e foi criado como forma de incitar ao desenvolvimento de aplicações e dispositivos sensoriais.

Os dispositivos denominados SunSpots foram construídos por forma a possibilitar a interacção com programadores que nunca tenham tido contacto com dispositivos embebidos, para que a interacção ultrapassasse os limites do rato, teclado e ecrã, para que as aplicações interajam não só com outras aplicações mas também com o seu ambiente.
Este projecto parte duma premissa declarada, "*Sun SPOTs are much more than just an embedded microprocessor that runs Java*", que expõe à partida uma quantidade de características que permitem aos Sun Spots aspirar a muito mais do que são conferindo-lhes um grau de versatilidade inigualável.

B.1 Capacidades Internas

Os dispositivos Sun Spot são compostos pelas seguintes capacidades:

Plataforma embebida de desenvolvimento - Hardware e software bastante flexíveis do ponto de vista do desenvolvimento.

Facilidade de Programar - Programação na linguagem Java.

Comunicação Wireless - Permite redes em *overlay* com suporte a CTP, IPv6/LowPan. Suporta também *mesh networks*, AODV, LQRP e *Multi-Hop Over the Air Programming*.

Mobilidade - Com uma bateria de iões de lítio carregada por USB tem uma autonomia considerável (ver B.2.3).

Segurança - Suporte para chave publica criptográfica ECC.

B.2 Arquitectura

O conjunto de desenvolvimento do projecto Sun Spot é composto por dois dispositivos SunSpot e uma basestation Sunspot como ilustrado na figura B.1.

Figura B.1: Kit Sun Spots.
Imagem retirada de `http://www.sunspotworld.com`

Os dispositivos SunSpot são compostos por uma placa de sensores embutida na placa do processador e uma bateria revestidos externamente por um corpo em plástico tal como ilustrado na figura B.2. A BaseStation é composta apenas por uma placa de processador revestida por um corpo de plástico.

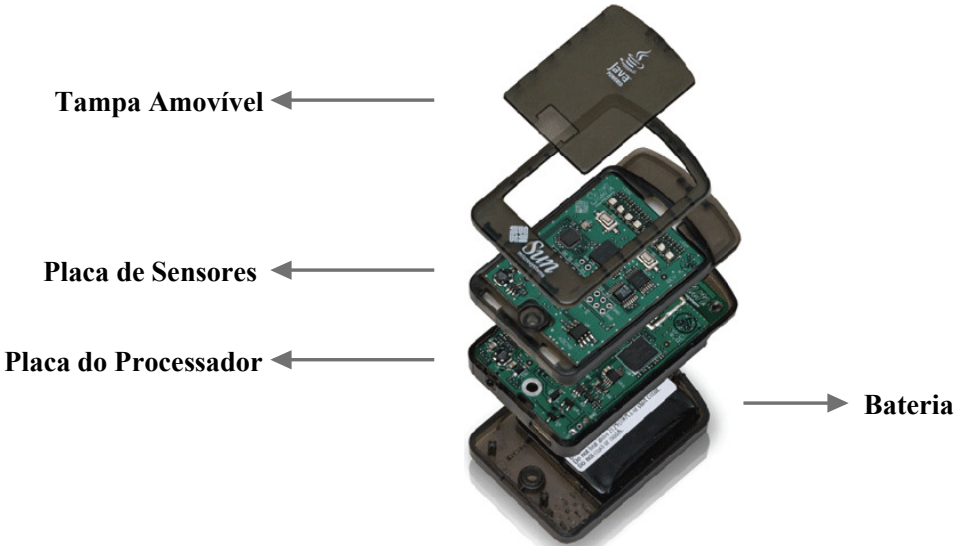


Figura B.2: Dispositivo Sun Spot.
Imagem retirada de `http://www.sunspotworld.com`

B.2.1 Capacidade de Processamento

Cada dispositivo/basestation é equipado com um processador ARM920T de 32 bits a 180MHZ e uma RAM de 512K com uma *flash* de 4M.

B.2.2 Conectividade

A placa de processamento dos elementos SunSpot contém um rádio de 2.4GHz com uma antena incorporada. O rádio é um TI CC420 e utiliza o protocolo de comunicação *standard* IEEE 802.15.4.

B.2.3 Autonomia

Cada dispositivo SunSpot é composto por uma bateria de 3.7V recarregável de iões de lítio que se recarrega cada vez que o elemento é ligado por USB a um computador ou *hub* de potência. A *basestation* não possui bateria uma vez que foi construída com o intuito de estar ligada a um terminal anfitrião.

Em funcionamento constante utilizando tanto o CPU como o rádio a bateria tem uma autonomia até 7 horas.

B.2.4 Sensores e Actuadores

Como já foi referido, os dispositivos SunSpot contém um conjunto de sensores de fácil acesso que permitem uma captura de informação de ambiente detalhada. De notar, que, além dos sensores embutidos, a placa suporta *pins* de expansão que permitem a ligação de todo o tipo de dispositivos, desde sensores, componentes robóticos, etc. De origem, os dispositivos são compostos por:

- Acelerómetro de 3 eixos com configuração de alcance para 2G e 6G.
- Sensor de Temperatura
- 8 Leds de três cores
- 6 inputs analógicos por ADC
- 2 interruptores(*momentary switches*)
- 5 *pins* IO de utilização geral
- 4 pins de output de alta corrente

B.2.5 Aplicações Práticas

O projecto SunSpot pode considerar que os seus objectivos foram cumpridos uma vez que existem neste momento aplicações para os Sun Spots tanto ao nível de software como hardware espalhadas por todas as áreas tecnológicas com um número de implementações interessante.

Sendo uma plataforma de fácil desenvolvimento e apresentando uma arquitectura orientada à investigação e exploração das áreas que compõe este projecto, estão espalhados pela internet infinitos códigos de programação e esquemáticos para implementação de novos sensores, novos componentes de integração de *hardware*, *etc.*. A figura B.3 demonstra um exemplo das várias aplicações físicas e inerente programação dos multi-usos destes dispositivos.

Figura B.3: Várias Aplicações para Sun Spot.
Imagem retirada de `http://www.sunspotworld.com`

Software

Os SunSpots não possuem sistema operativo, todo o *software* opera com base numa *Java Virtual Machine* directamente implementada. Utilizam uma implementação de de Java ME chamada Squawk que suporta CLDC 1.1 e MIDP 1.0 e além disso fornece funcionalidades básicas de sistema operativo. A virtual machine é executada directamente a partir da memória *flash* e todos os *drivers* são escritos em Java. Todo o *software* disponibilizado pela Sun Spot é o*pen source com* licença GNU GPL v2.0.

B.2.6 Desenvolvimento

Este equipamento foi desenvolvido em orientação à criação de um infindável número de aplicações. Para desenvolvimento de software podem ser utilizados vários IDEs, no entanto existe uma integração optimizada com o NetBeans para criação e *deployment* de código.

Apêndice C

PT Context Broker

O PT Context Broker é um projecto da Portugal Telecom em colaboração com o Instituto de Telecomunicações de Aveiro que visa a criação de um *context broker*.

Um **context broker** é composto por um servidor XMPP *context aware* em conjunto com uma camada de inteligência formada a partir da informação que obtém. Essa camada de inteligência permite-lhe tomar decisões e efectuar operações ao nível dos componentes que o integram e dos elementos que a este se conectam.

O seu funcionamento isolado não produz resultados. O *Context Broker* tem como função recolher informações a partir de *Context Providers* e fornece-as a *Context Consumers*

Os **context providers** são a fonte de informação de todo este sistema. São todos os elementos que injectam informação dos mais variados formatos e origens. Uma das grandes vantagens e é também o que enriquece a camada de inteligência do CxB é o facto da origem da informação poder ser baseada em praticamente qualquer fonte, desde sensores (e.g. sensores de temperatura, de presença, de aceleração, etc) a informação retirada de serviços (e.g. Google Calendar, Google Address Book, *etc.*) e até informação baseada em localização(e.g. Google Maps, GPS, *etc.*).

Context consumers são os utilizadores finais de toda a informação acumulada e podem ser aplicações simples ou incorporar aplicações complexas. Os CxC podem descobrir e subscrever informação/serviços disponibilizados pelo CxB para realizar operações ponderadas pelo que se pode inferir que quanto mais e melhor informação se possuir mais consciente será a decisão.

A figura C.1 representa um modelo conceptual de relações entre as três entidades, CxC, CxB e CxP. Como ilustrado um CxC pode ser qualquer tipo de terminal que possua uma aplicação que vá requerer junto do CxB a informação que melhor lhe aprouver. Os CxP tal como exemplificado podem gerar informação de múltiplas origens e formatos.

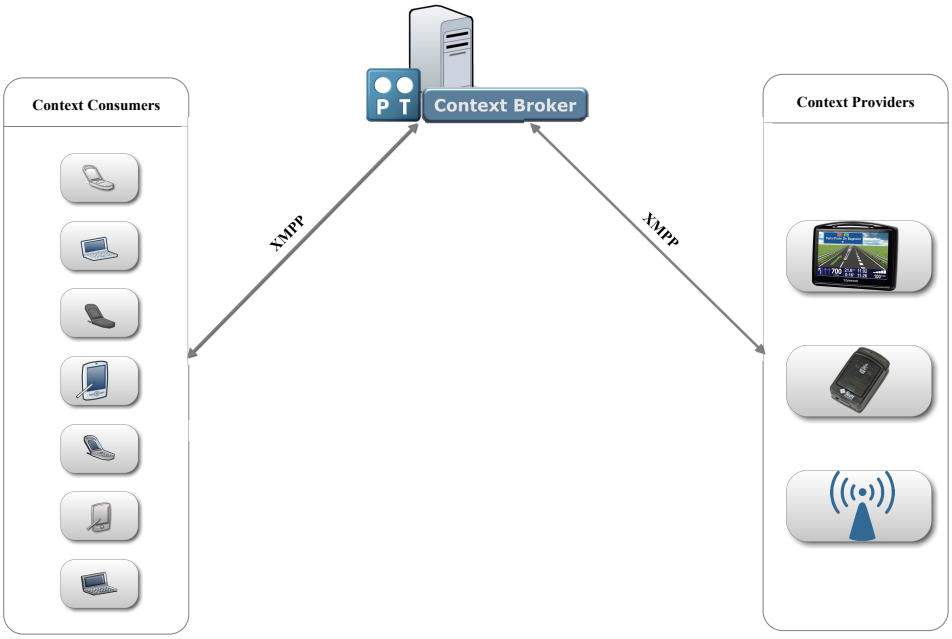


Figura C.1: Modelo conceptual de contexto

C.1 Arquitectura

O *context broker* é composto internamente por quatro elementos, dois serviços e dois modelos de dados. Os dois serviços implementados são o serviço de publish-subscribe comummente conhecido por PubSub e o serviço de descoberta. Os modelos de dados que compõe o *context broker* são o histórico de contexto e a cache de contexto.

A figura C.2 demonstra conceptualmente a arquitectura implementada pelo PT Context Broker.

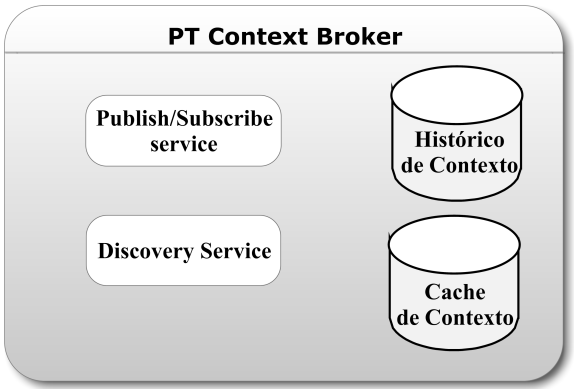


Figura C.2: Modelo conceptual do context broker

O **PubSub** é um serviço de tempo real que suporta a publicação e subscrição de conteúdos na web. É composto por nós de conteúdos, os CxP injectam informação para os nós respectivos

e os CxC subscrevem os nós cuja informação lhes interessa e cada vez que a informação é actualizada é enviada ao CxC uma mensagem com os dados actualizados.

O **serviço de descoberta** é um mecanismo que permite às entidades descobrirem informação sobre as entidades da rede bem como serviços (PubSub) e os seus nós de dados disponíveis.

Como forma de suporte aos serviços prestados o PT Context Broker dispõe de dois modelos de dados. O **histórico de context** permite ao CxB fornecer aos seus CxC informação não só sobre os dados actuais mas também sobre informação passada.

A **cache de contexto** permite ao CxB armazenar em cache um conjunto de informações mais requeridas pelos consumidores reduzindo assim o tempo de acesso e serviço em detrimento de fazer o *fetch* dos dados constantemente à base de dados ou aos CxP.

Apêndice D

Pachube

Pachube é um *website* que providencia um *webservice* em `http://www.pachube.com` que permite guardar e partilhar informação dos mais variados tipos de sensores espalhados por todo o mundo. É uma plataforma segura e escalável que permite a interligação de contextos sensoriais e permite o acesso à sua informação, graficamente através do Google Maps e programaticamente através de *webservices*.

Actuando como intermediário entre os vários sensores que estão conectados permite uma captura de dados constante e disponibiliza os mesmos para acesso externo a utilizadores remotos. Esta plataforma permite aos utilizadores monitorizarem e partilharem dados em tempo real facilitando a interacção entre sistemas/ambientes remotos. Além de permitir ligação entre dois sistemas permite ainda estabelecer ligações *many-to-many* interligando um grande número de entidades de forma transparente. A figura D.1 ilustra os vários tipos de relações existentes e suportadas pelo Pachube.

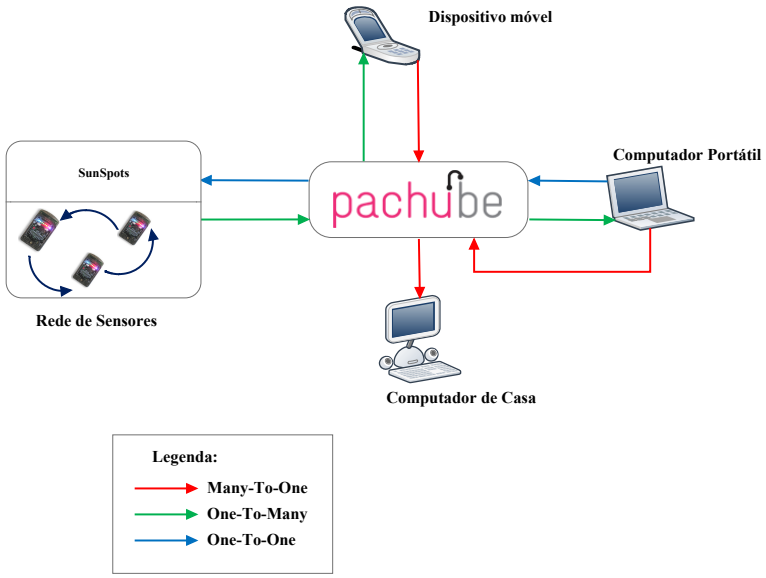


Figura D.1: Diagrama de Relações

D.1 Aplicações por medida

O Pachube disponibiliza bibliotecas de funções que tornam a construção de aplicações e serviços de forma bastante fácil e intuitiva. Por este motivo o Pachube tem vindo construir o seu lugar no mundo dos sensores e partilha de informação de contexto e tem sido incluído em diversos sistemas, desde aplicações de monitorização remota, integração em sistemas de gestão de edifícios, sistemas de *geo-tracking*, criação de redes e *mashups* de objectos, sistemas de *logging* de sensores, *etc.*.

D.2 Arquitectura

Existem várias formas de aceder e guardar informação no Pachube, manualmente e automaticamente. Manualmente, é o utilizador que faz *push* através de HTTP PUT *request* da informação que possui enquanto que automaticamente é o Pachube que tendo acesso constante à informação dos sensores faz *push* para ele próprio quando achar que o deve fazer.

O Pachube utiliza, como forma de comunicação e transporte de dados, algumas tecnologias como o XML(em formato EEML), CSV, JSON, RSS e Atom. O suporte aos vários formatos é conseguido utilizando uma API RESTful extensiva. No entanto, nem todos os métodos de *request* suportam todos os formatos.

D.2.1 Formatos de Dados

EEML - Este formato contém o mais completo conjunto de dados. Permite a definição de metadados incluindo *tags* para cada *datastream* interiormente à aplicação utilizada.

JSON - À semelhança do EEML também contém todos os elementos de dados disponíveis.

CSV - Tipicamente é o formato que contém menos informação. É formado por valores separados por virgulas e só contem os valores dos ultimos *updates* em cada *datastream*. No entanto é o formato que permite mais rapidez e simplicidade.

RSS e Atom - Estes formatos contém os titulos dos *feeds*, IDs e localização geográfica.

Outros detalhes que dizem respeito à formatação de dados estão disponíveis no *website* do Pachube. [28]

D.2.2 Http Requests

Existem alguns métodos de HTTP *Request* que permitem a interacção com o *website*.

GET - Método que permite a obtençao de dados a partir da API Pachube.

PUT - Actualização e edição de dados do *feed* é feita através do método PUT.

DELETE - Este método permite eliminar um *feed*.

D.2.3 Autenticação

Praticamente todos os métodos de tempo real utilizados requerem chave de API. Esta chave é passada através do cabeçalho do HTTP *request* ou como parâmetro "*key*"no URL.

D.2.4 Segurança

O Pachube suporta conecções SSL verificando a identidade do elemento com que se comunica. Se por algum motivo a segurança for um factor de preponderante então o acesso ao *website* pode ser feito utilizando "https://"em detrimento do "http://".

D.2.5 Organização de Dados

Os dados estão internamente organizados por *feeds*. Cada feed possui características, que de todas, apresentam-se as mais relevantes:

Tipo - Define o tipo de feed como sendo automático ou manual. O tipo manual permite ao utilizador decidir quando fazer a actualização de dados. O tipo automático transfere a responsabilidade de actualização de dados para o próprio Pachube.

Titulo - Nome pelo qual o feed ficará conhecido

Localização - Esta característica é composta por seis atributos. O nome da localização, a elevação em metros, a exposição definindo se é um sensor interno ou externo a um edifício, a disposição, que especifica se o sensor é fixo ou móvel, o domínio da sua existência, se físico se virtual. O ultimo atributo do *feed* é a localização através do Google Maps que permitirá mais tarde, através do *website* localizar o *feed* através de um marcador escolhido e colocado por este atributo.

Datastream - Cada feed pode ter vários *datastreams*. Um *datastream* é composto por cinco atributos relaccionados com o tipo de sensor em questão. o ID que identifica o *datastream*, uma *tag* que pode ser utilizada ou não e tipicamente é utilizada pelas aplicações como forma de selecção interna, as unidades respectivas à medição que se está a obter, o símbolo correspondente a essas unidades e o tipo de sensor.

D.2.6 Taxa Limite

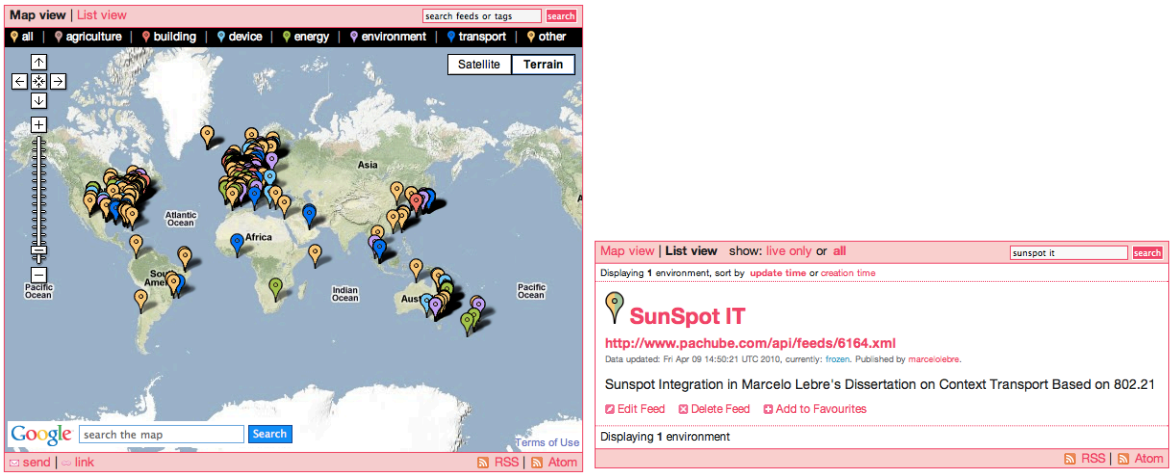
As chamadas à API do Pachube encontram-se limitadas até um máximo de 50 *requests* a cada 3 minutos. Se por algum motivo a aplicação violar esta taxa será impedida de efectuar *requests*, seja para aceder a dados ou actualizar dados. Assim que a taxa de *requests* gerada pela aplicação reduzir para um número aceitável as permissões serão repostas pelo serviço.

D.3 O Web Site

O *website* `www.pachube.com` está relativamente bem organizado e permite uma utilização bastante fluída e intuitiva. São disponibilizados ao utilizador vários tutoriais e documentação sobre a utilização e desenvolvimento de *software* recorrendo a APIs do Pachube.

Para se poder fazer uma utilização activa de todas as potencialidades é necessário um registo que além de grátis é bastante simples. Após registo cada utilizador tem uma conta que utiliza para efectuar todas as operações que necessita, criar *feeds*, editar *feeds*, gerir configurações, etc. No entanto, é possível consultar o *website* sem um prévio registo, fazendo por isso uma utilização passiva com um teor meramente de consulta do conteúdo informativo. A página inicial é composta por uma *mapview* do Google Maps com um grande número de

marcadores, cada marcador representa um *feed* de sensores. Os sensores estão divididos por categorias pelo que seleccionando a categoria que se pretende através de um painel superior à *mapview* todos os restantes *feeds* de sensores que não correspondem a essa categoria são retirados da vista actual. A figura D.2a representa a imagem inicial e a figura D.2b representa a opção de procura por lista, que, em caso de existirem vários resultados permite uma melhor distinção.

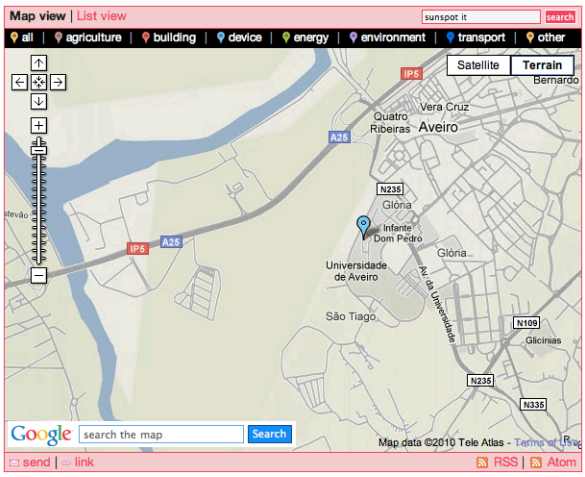


(a) Pachube MapView

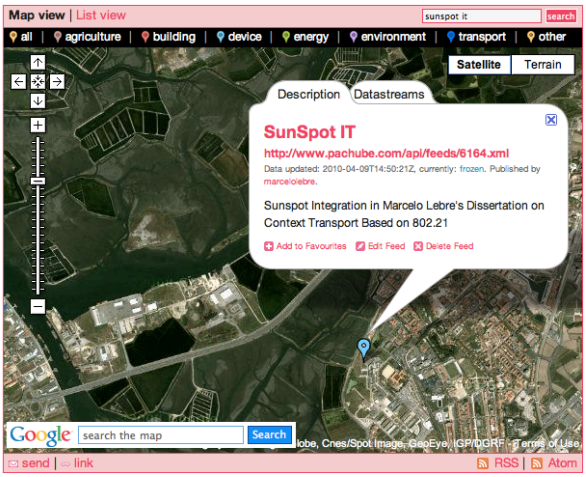
(b) Pachube ListView

Figura D.2: Views diferentes no Pachube.
Imagens retiradas de `http://www.sunspotworld.com`

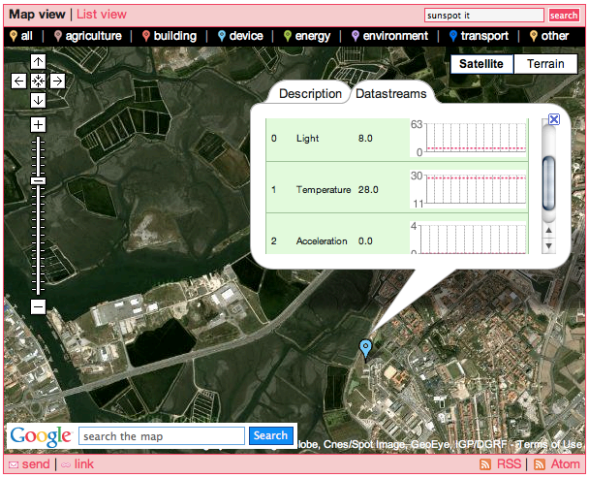
Após selecção do *feed* que queremos consultar é aberta uma pequena janela sobre o mesmo, com dois separadores, o primeiro, representado na figura D.3b Description aparece o nome do *feed*, o URL para acesso com o ID, o estado, o autor da publicação e uma breve descrição feita pelo utilizador aquando da criação do mesmo. O segundo separador, ilustrado pela figura D.3c, Datastreams, representa os tipos de sensores associados ao *feed*, os últimos valores associados e um pequeno gráfico individual com o historial das últimas 24 horas.



(a) IT no Pachube



(b) Pachube Feed



(c) Pachube Datastream

Figura D.3: Feeds e Datastreams.
Imagens retiradas de `http://www.pachube.com`

Apêndice E

Mensagens XMPP

E.1 Obtenção de informação de nós

```
<iq type="get" to="pubsub.c3s.av.it.pt" id="info2">
    <query xmlns="http://jabber.org/protocol/disco#info"node="sensornetworks:32DE"/>
</iq>
```

E.2 Criação de nós

E.2.1 Criação de um nó do tipo Collection

```
<iq type="set" to="pubsub.c3s.av.it.pt"  id="create3">
  <pubsub xmlns="http://jabber.org/protocol/pubsub">
    <create node="sensornetworks:32DE"/>
    <configure>
      <x xmlns="jabber:x:data" type="submit">
        <field var="FORM_TYPE" type="hidden">
          <value>http://jabber.org/protocol/pubsub#node_config</value>
        </field>
        <field var="pubsub#node_type"><value>collection</value></field>
      </x>
    </configure>
  </pubsub>
</iq>
```

E.2.2 Criação de um nó do tipo Leaf

```
<iq type="set" to='pubsub..c3s.av.it.pt" id="create4">
  <pubsub xmlns="http://jabber.org/protocol/pubsub">
    <create node="sensornetworks:32DE"/>
    <configure>
      <x xmlns="jabber:x:data" type="submit">
        <field var="pubsub#collection"><value>sensornetworks</value></field>
      </x>
    </configure>
  </pubsub>
</iq>
```

E.3 Subscrição

```
<iq type="set" to="pubsub.c3s.av.it.pt" id="sub1">
    <pubsub xmlns="http://jabber.org/protocol/pubsub">
        <subscribe node="sensornetworks:32DE" jid="sensor21@c3s.av.it.pt"/>
    </pubsub>
</iq>
```

E.4 Publicação

```
<iq type="set" id="611-220" to="pubsub.c3s.av.it.pt" from="sensornetworks.c3s.av.it.↩
    pt">
  <pubsub xmlns="http://jabber.org/protocol/pubsub">
    <publish node="sensornetworks:32DE">
      <item xmlns="">
        <sensor21>
          <light>10</light>
          <temperature>28</temperature>
          <acceleration>0</acceleration>
        </sensor21>
      </item>
    </publish>
  </pubsub>
</iq>
```

E.5 Actualização de dados

```
<message from="pubsub.c3s.av.it.pt" to="sensor21@c3s.av.it.pt" id="foo">
  <event xmlns="http://jabber.org/protocol/pubsub#event">
    <items node="sensornetworkis:32DE">
      <item id="ae890ac52d0df67ed7cfdf51b644e901">
       <sensor21>
          <light>10</light>
          <temperature>28</temperature>
          <acceleration>0</acceleration>
        </sensor21>
      </item>
    </items>
  </event>
</message>
```